УДК 004.932.72'1

О.В. НЕЧИПОРЕНКО, Я.В. КОРПАНЬ
Черкаський державний технологічний університет

БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ І АВТЕНТИФІКАЦІЯ ОСОБИ ЗА ГЕОМЕТРІЄЮ ОБЛИЧЧЯ

В статті наведені результати аналізу методів розпізнавання обличчя та алгоритмів порівняння шаблонів образів, а також огляд сучасних систем розпізнавання особи за геометрією обличчя і виявлення сфер використання і тенденцій розвитку систем біометричної ідентифікації та автентифікації осіб за геометрією (формою) обличчя.

Ключові слова: ідентифікація, автентифікація, метод, біометрична система, геометрія обличчя.

O.V. NECHYPORENKO, Y.V. KORPAN
Cherkassy State Technological University

BIOMETRIC IDENTIFICATION AND AUTHENTICATION OF PERSONS FOR GEOMETRY FACE

The article presents an analysis of facial recognition methods and algorithms compare the template images and an overview of modern systems for facial recognition facial geometry. Identified areas of use and trends of biometric identification and authentication of persons by geometry (shape) of the face. One of the most promising biometrics market trends is the emergence of intelligent digital camcorders that implement face detection based on embedded logic. Modern facial recognition systems face are used not only to detect serious problems such wanted persons in public places, but also for purely civilian purposes. Analysis of the most popular programs shows that they have very little chance of error, provide comfort. Their characteristics are about the same and the choice depends on personal requirements of the user.

Keywords: identification, authentication method, biometric system, the geometry of the face.

Вступ

Впровадження біометричних систем в життя суспільства є незаперечним фактом. Світові аналітики прогнозують підвищення попиту на біометрії в усіх галузях і розширення сфери її застосування.

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; інформаційна безпека; облік робочого часу та реєстрація відвідувачів; системи голосування, проведення електронних платежів; автентифікація на Web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідування країни).

Ідентифікація на основі біометричні данні – це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних [1].

Для користувачів, які застосовують системи біометричної ідентифікації і автентифікації, дуже важливим є зручність застосування цих засобів (це не тільки швидкість і простота проведення процедури, але і можливість використання звичного обладнання). На сьогодні оптимальним співвідношенням між надійністю автентифікації, ціною і зручністю використання має визначення особистості по обличчю, чим і пояснюється високий темп розвитку і поширення таких технологій.

Аналіз досліджень та публікацій

Інтеграція України до Європи зачіпає не лише економічну і політичну, але і соціальну сферу життя наших громадян. Європейський союз визначив набір протоколів для реалізації ЕАС (доступу до критичних даних (біометричних даних) в своїх електронних паспортах (ЕП, ePassport)). В Україні і в країнах ЄС ведеться робота по впровадженню біометричних паспортів [1].

Так, згідно з Концепцією створення національної системи ідентифікації громадян України, іноземців та осіб без громадянства основними напрямами реформи є [2]:

- запровадження системи достовірної ідентифікації особи і встановлення її законних даних; створення електронних баз даних; усунення випадків дублювання і незаконної зміни даних; використання інформаційних технологій для ідентифікації особи, перевірки даних і ефективного аналізу баз даних; впровадження сучасних технічних засобів;
- запровадження сучасних та захищених ідентифікаційних документів. Одним з важливих чинників є визначення фізичних і функціональних характеристик документа, що посвідчує особу, його значення у контексті електронного урядування, у тому числі цифрового підпису;
- надання високоякісних, прозорих, безпечних та швидких послуг суб'єктам звернення.

Основними джерелами з питань біометричного паспорту є різноманітні публікації організації цивільної авіації ІСАО. Це, в першу чергу, Doc 9303, що складається з кількох частин. Основоположною є частина 1 «Машинозчитуємі паспорти» том 2 «Специфікації на електронні паспорти з засобами біометричної ідентифікації» [1].

Метою статті є аналіз методів розпізнавання обличчя та алгоритмів порівняння шаблонів образів, а також огляд сучасних систем розпізнавання особи за геометрією обличчя і виявлення сфер використання і

тенденцій розвитку систем біометричної ідентифікації та автентифікації осіб за геометрією (формою) обличчя.

Матеріали досліджень

1. Загальні відомості про біометрію обличчя

Розпізнавання обличчя – найбільш древній і поширений спосіб ідентифікації, заснований на тому, що риси обличчя і форма черепа кожної людини індивідуальні. Комп'ютер лише автоматизує процедуру, виконуючи аналогічну процедуру, з тією різницею, що замість фото застосовуються біометричні дані, записані в еталонному образі. Так як використовуються фізіологічні характеристики людини, цей метод відноситься до статичних методів біометрії. Це самий інтуїтивно зрозумілий метод ідентифікації, найбільш близький до того, як люди ідентифікують один одного.

Необхідно відзначити, що останнім часом розроблені деякі інші методи розпізнавання, що виконують сканування обличчя, наприклад, розпізнавання облич в інфрачервоному світлі по термограмі обличчя. У зв'язку з цим назву методу уточнюють – називають його ідентифікацією за геометрією обличчя.

Розпізнавання за рисами обличчя має ряд переваг перед іншими біометричними технологіями:

- не потрібно безпосереднього контакту людини, обличчя якої встановлюють, зі сканером, за винятком систем розпізнавання облич в складі стандартних електронних охоронних систем, де людина при верифікації дивиться прямо в камеру;
- при відповідному обладнанні розпізнавання за рисами обличчя можливо на значній відстані, в групі людей, не привертаючи уваги;
- це єдиний біометричний спосіб ідентифікації з точки зору можливості багатоцільового застосування, не вимагає спеціальної техніки;
- при ідентифікації використовується загальнодоступна біометрична характеристика, зазвичай не приховувана людиною.

Будь-яка система розпізнавання обличчя – це типова система розпізнавання образів, завдання якої зводиться до формування деякого набору ознак, так званого біометричного шаблону, згідно закладеної в систему математичної моделі. Розпізнавання обличчя в будь-якій біометричній системі виконується в кілька етапів: виявлення обличчя, оцінка якості, побудова шаблону, зіставлення і прийняття рішення [3].

1. На етапі виявлення обличчя система автоматично визначає в потоці відеокадрів або на фотографії обличчя людей, причому діапазон ракурсів і масштабів осіб може значно варіюватися, що вкрай важливо для побудови систем безпеки. Виявлення обличчя є одним з ключових етапів розпізнавання, так як пропуск особи детектором автоматично означає неможливість подальшої ідентифікації. Якість роботи детектора прийнято характеризувати ймовірністю виявлення особи. Для сучасних біометричних систем, що працюють в умовах потоку людей, значення ймовірності виявлення особи становить від 95 до 99% і залежить від умов реєстрації відео (освітленість, роздільна здатність і т.д.).

2. На етапі оцінки якості здійснюється вибір з усього масиву виділених облич тільки тих зображень, які задовольняють заданим критеріям якості. На практиці системи біометричної ідентифікації змушені мати справу з не дуже сприятливими умовами роботи: відхилення обличчя від фронтального положення на кути, що перевищують 20 град.; сильне засвічування; перекриття частини обличчя; наявність тіней на обличчі; малий розмір зображення і т.п. Саме стабільність роботи біометричної системи в таких складних умовах і визначає її якість. Як правило, оцінюються: ракурс обличчя (не повинен перевищувати 20–30 град.); розмір обличчя (оцінюється за відстанню між зіницями очей і повинен бути більше 50–80 пкс); часткове закриття обличчя (закриття не повинно бути більше 10–25% від загальної площі обличчя).

3. Побудова шаблону – це один з найбільш складних і унікальних етапів розпізнавання обличчя, що становить ключове досягнення новітніх технологій. Суть даного етапу полягає в нетривіальному математичному перетворенні зображення обличчя в набір ознак, об'єднаних в біометричний шаблон. Принципи побудови біометричних шаблонів надзвичайно різноманітні. Найважливішою характеристикою біометричного шаблону є його розмір. Чим більше розмір шаблону, тим більше інформативних ознак він включає в себе, але тим нижче швидкість і ефективність пошуку цього шаблону.

4. Зіставлення і прийняття рішення – це об'єднаний етап роботи системи розпізнавання, на якому проводиться порівняння біометричного шаблону обличчя, побудованого за виділеним обличчям, з масивом шаблонів. У найпростішому випадку зіставлення здійснюється простим перебором всіх шаблонів і оцінкою міри їх схожості. На підставі отриманих оцінок і їх зіставлення з заданими порогами приймається рішення про наявність чи відсутність ідентичної особи в базі даних. У сучасних системах зіставлення реалізується за складними оптимальними схемами порівняння, що забезпечує швидкість зіставлення від 10 000 до 200 000 порівнянь в секунду і більше. Процес порівняння може бути розпаралеленим, що дозволяє працювати системам ідентифікації практично в режимі реального часу навіть по великих масивах зображень.

Ефективність роботи алгоритму стосовно заданого біометричного параметру зазвичай оцінюють за двома критеріями [6]:

- FAR (False Acceptence Rate) – коефіцієнт помилкового доступу, процентний показник випадків, при яких перевірка особи виявилася помилково успішною.
- FRR (False Rejection Rate) – коефіцієнт помилкової відмови в доступі, процентний показник випадків, при яких перевірка особи помилково завершилася невдачею.

Теоретично система тим краще, чим менше значення FRR і FAR. Однак, в більшості випадків більш

важливою є якась одна з величин. Зокрема, для системи контролю логічного або фізичного доступу пріоритетом є заборона доступу не уповноважених осіб за будь-яких обставин, як більш критичної обставини. Очевидно, що для цього необхідний дуже низький FRR. Залежно від конкретного завдання можливе настроювання на певний компроміс між припустимими значеннями FRR і FAR, або, як їх прийнято називати в теорії статистичних рішень, помилками 1-го й 2-го роду.

Ефективність розпізнавання обличчя безпосередньо залежить від таких факторів, як стійкість біометричного шаблону до різного роду перешкод, спотворень у вихідному фото- або відеозображенні [3–5].

Надійність роботи системи розпізнавання осіб залежить від декількох факторів [7]:

- якість зображення (помітно знижується ймовірність безпомилкової роботи системи, якщо людина, яку ми намагаємося ідентифікувати, дивиться не прямо в камеру або знята при поганому освітленні);
- актуальність фотографії, занесеної до бази даних;
- величина бази даних (обсяг баз даних при використанні стандартних персональних комп'ютерів не перевищує 10000 зображень).

Якість роботи систем розпізнавання осіб прийнято характеризувати ймовірностями ідентифікації. Хоча обличчя людини і унікальний параметр, але мінливий – риси обличчя змінюються в залежності від повороту голови, психологічного стану, мімічного вираження, наявності бороди, вусів, окулярів, косметики. Щоб забезпечити високу надійність впізнання незалежно від цього, кількість, якість і різноманітність зчитувальних образів може варіюватися в залежності від алгоритмів і функцій системи, що реалізує даний метод.

2. Технології біометрії за формою обличчя і алгоритми порівняння шаблонів

В даний час існує чотири основні методи розпізнавання особи, які розрізняються складністю реалізації та метою застосування [7]:

- метод автоматичної обробки зображення особи;
- «eigenfaces» (нім. «власне обличчя»);
- аналіз відмінних рис;
- аналіз на основі нейронних мереж.

Метод автоматичної обробки зображення обличчя – найбільш проста технологія, що аналізує відстані і відношення відстаней між легко визначеними точками обличчя. Особливо важливі характерні частини обличчя, а також ті, які практично не змінюються з плином часу: очі, вилиці, кінець носа, куточки рота. Хоча даний метод не дуже потужний, він може бути досить ефективно використаний в умовах слабкої освітленості.

Технологія «eigenface» використовує представлення зображення обличчя в градаціях сірого у вигляді статистично обґрунтованих, стандартних блоків даних (областей обличчя). Даний метод заснований на тому, що всі обличчя можуть бути отримані з репрезентативної вибірки облич з використанням сучасних статистичних прийомів. Вони охоплюють пікселі зображення обличчя і універсально представляють форми обличчя (двомірні зображення-шаблони). Комбінуючи 100–120 різних шаблонів, можна представити велику кількість облич. При реєстрації вигляд кожної конкретної людини представляється рядом коефіцієнтів, що вказують найбільш відповідні шаблони. Для режиму встановлення автентичності, коли проводиться перевірка ідентичності, біометричний образ користувача обробляється і порівнюється з раніше зареєстрованим набором коефіцієнтів, з метою визначення коефіцієнта відмінності. Ступінь відмінності між шаблонами і визначає факт ідентифікації. Технологія «eigenface» оптимальна в добре освітлених приміщеннях, при можливості сканування особи в фас. Метод використовується в якості основи для інших методів розпізнавання особи.

Методика аналізу відмінних рис подібна методиці «eigenface», але в більшій мірі адаптована до зміни зовнішності або міміки людини. У технології аналізу відмінних рис використовуються не тільки характерні особливості областей обличчя, а й враховано їх відносне положення. Тобто ідентичність обличчя визначається не тільки характерними елементами, але і способом їх геометричного об'єднання. Індивідуальна комбінація цих параметрів визначає особливості кожного конкретного обличчя.

У методі, заснованому на нейронних мережах, характерні особливості зареєстрованого і перевіряємого облич порівнюються на співпадіння. Нейронні мережі встановлюють відповідність унікальних властивостей людини, а потім за допомогою відповідних вагових коефіцієнтів кожної характеристики визначається ступінь загальної відповідності обличчя до еталону. Метод має високу якість ідентифікації в складних умовах.

Для порівняння з графічними зображеннями-шаблонами застосовуються два основних алгоритми: мінімальної середньої кореляційної енергії (MACE) [6] і локальні бінарні шаблони (LBP) [9].

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 інваріантним 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 ступеня кореляції. Для забезпечення більшої надійності в базі потрібно мати порівняно велику кількість зображень обличчя, в різних умовах освітлення і зміни міміки.

3. Методи розпізнавання особи

Вся множина методів розпізнавання за геометрією обличчя ділиться на два напрямки: 2D і 3D методи розпізнавання [10]. У кожного з них є переваги і недоліки, проте багато що залежить ще і від області застосування і вимог, пред'явлених до конкретного алгоритму.

3.1 Розпізнавання обличчя в 2D

Цей напрямок ідентифікації з'явилося давно і бере початок в криміналістиці. Розпізнавання обличчя спочатку мало низьку в порівнянні з іншими методами надійність. Високі результати досягалися лише при фіксованих зовнішніх факторах (ракурс, освітленість, дальність і т.п.). В даний час він застосовується лише в багатофакторній (перехресній) автентифікації, або в соціальних мережах (вказівка людей на фото в Facebook). В задачах ідентифікації при використанні великих баз даних надійність і швидкодія таких біометричних систем різко знижується, змушуючи використовувати додаткові ознаки для автентифікації. На практиці також пред'являються вимоги до освітлення, відсутності зовнішніх перешкод. Обов'язкове фронтальне зображення обличчя з досить невеликими відхиленнями, багато алгоритмів не враховують можливі зміни міміки обличчя. Все це додає труднощів при ідентифікації і встановлює певні мінімальні вимоги до обчислювальної потужності апаратури. На практиці досить стандартних відеокамер з роздільною здатністю 320x240 ppi, які передають дані зі швидкістю відеопотоку, принаймні 3–5 кадрів в секунду. Інтенсивний розвиток і, як наслідок, здешевлення цифрового відео і мультимедійних цифрових технологій дозволяють впровадити їх в широке використання. Найбільш поширеними пристроями, що дозволяють отримати двомірне зображення обличчя користувача є веб-камери.

2D система працює з відносно простим двовимірним зображенням, що помітно спрощує алгоритми і знижує інтенсивність обчислень. Переваги методу 2D розпізнавання обличчя: не потрібне дороге обладнання; при відповідному обладнанні можливість розпізнавання на значних відстанях від камери. Недоліки: низька статистична достовірність; вибагливість до освітлення; неприйнятність будь-яких зовнішніх перешкод; не враховують можливі зміни міміки обличчя, вираз повинен бути нейтральним [1].

Сучасні алгоритми здатні компенсувати наявність окулярів, вусів і бороди, а також додаткових аксесуарів на обличчі досліджуваної людини навіть на двомірному зображенні. Однак основною проблемою використання двомірних зображень є вразливість до атак з використанням муляжів. Для обману таких систем досить використання фотографії суб'єкта.

3.2 Розпізнавання обличчя в 3D

Реалізація являє собою досить складне математичне і технічне завдання. В даний час існує багато методів по 3D розпізнаванню обличчя. Методи неможливо порівняти один з одним, так як вони використовують різні сканери та бази, не для всіх з них вказані FAR і FRR, використовуються абсолютно різні підходи.

Класичним є метод проектування шаблону. Він полягає в тому, що на обличчя проектується світлова сітка. Промінь, що падає на викривлену поверхню, згинається – чим більше кривизна поверхні, тим сильніше вигин променя. Спочатку застосовувалося джерело видимого світла, а потім – інфрачервоне. Камера робить знімки зі швидкістю десятки кадрів в секунду, а отримані зображення обробляються спеціальною програмою. За отриманими знімками відновлюється 3D модель обличчя, на якій виділяються і видаляються непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі – виділяються антропометричні особливості, які записуються в унікальний код, що заноситься в базу даних. Крім низької чутливості до зовнішніх чинників, найважливішою перевагою методу є високий рівень надійності.

Переваги методу 3D розпізнавання обличчя: висока достовірність розпізнавання – більше інформації, ніж має звичайний знімок; стійкість розпізнавання до відхилення ракурсу особи від фронтального; стійкість розпізнавання до неоднорідності освітлення; відсутність необхідності контактувати з пристроєм; низька чутливість до зовнішніх факторів. Недоліки: має обмежену сферу застосування із-за поганих статистичних показників; дороге обладнання; зміна міміки обличчя і перешкоди на обличчі погіршують статистичну надійність методу [1].

Досить надійні системи базуються на застосуванні декількох камер, розташованих під різними кутами і забезпечують формування тривимірної моделі обличчя. У них також використовується додаткове підсвічування для зниження впливу освітлення на одержуваний результат. Подібні системи знаходять застосування на контрольно-пропускних пунктах. У той же час застосування таких систем звичайними користувачами в повсякденних умовах неможливо через їх високу вартість, складності установки і використання [6].

В роботі [10] детально розглянуто методи, що базуються на автентифікації особи за геометрією обличчя. Результати аналізу представлено у вигляді 10-бальної шкали (чим ближче оцінка до 10, тим краще система). Для методу ідентифікації за геометрією обличчя з використанням двох вимірів FAR становить 0,1–0,001%, FRR – 2,5–9,0%, а з використанням трьох вимірів FAR становить 0,0047%, FRR – 0,103%.

4. Аналіз ринку систем розпізнавання особи за геометрією обличчя

В області розпізнавання 2D обличчя основним предметом розробки є програмне забезпечення:

алгоритми обробки і формування біометричного образу набувають переважаючий вплив на точність розпізнавання. У рішенні задачі розпізнавання по зображенню обличчя протягом декількох років практично не відбувається поліпшення статистичних показників алгоритмів.

3D розпізнавання обличчя зараз є більш привабливою областю для розробників. На сьогоднішній день розроблено цілий ряд комерційних продуктів, призначених для розпізнавання обличчя. Алгоритми їх різні і складно оцінити, яка з технологій має перевагу. Досить широкий і спектр застосування систем з розпізнаванням форми обличчя: від систем контролю доступу до систем автоматизованого документообігу.

Як приклад діючої системи контролю доступу на базі розпізнавання обличчя можна привести систему TrueFace компанії "Miros" для розпізнавання відвідувачів кіосків для переведення в готівку чеків у кількох штатах США. Також в цій країні застосовують автоматизовану систему сканування фотографій для водійських посвідчень. Найбільш продавана в Європі система контролю доступу – ZN-Face компанії "ZN Vision Technologies AG", сертифікована Німецьким відомством інформаційної безпеки. Спочатку розроблена для атомних електростанцій, вона тепер застосовується як європейським відділенням корпорації Microsoft в Німеччині, так і спортивними клубами в Голландії. ZN-Phantomas – це база фотоданих, автоматично порівнює і ідентифікує обличчя, використовується поліцією в Європі і США для розшуку злочинців, зниклих людей і впізнання жертв.

Система розпізнавання по обличчю FaceIt, розроблена компанією "Visionics", має складний математичний код індивідуальної ідентичності, який може бути порівняний з іншими з феноменальною точністю, незалежно від змін у освітленні, тону шкіри, окулярів, виразу обличчя, волосся на обличчі та голові, стійкий до зміни ракурсу. У Великобританії FaceIt інтегрована в телевізійну антикримінальну систему Mandrake, яка шукає злочинців по відеоданих 144 камер, об'єднаних в мережу.

Також успішне розпізнавання осіб застосовується в системах моніторингу робочого часу. Подібні системи все більш затребувані на ринку. Про ефективність біометричних систем обліку робочого часу свідчить і досвід світових компаній. Наприклад, мережа ресторанів "McDonald's", яка впровадила біометричну систему обліку робочого часу, змогла заощадити більше 20% фонду заробітної плати в Венесуелі.

Компанія "Google" відмічає привабливі перспективи інтеграції подібних технологій в свої сервіси для роботи з графічною інформацією. Ефективне розпізнавання облич було б дуже корисно в усьому, що стосується організації цифрових фотоальбомів і швидкого пошуку фотографій в них. Агентство "Reuters" оголосило про те, що має намір вбудувати в свій новий сайт програму відеопошуку. У поєднанні з Viewdle, засобом розпізнавання облич, програма "Reuters" індексує відеоматеріали агентства, так що найближчим часом користувачі отримають можливість шукати відеосюжети, які містять конкретних людей.

Найпростіші функції розпізнавання осіб реалізовані в цифрових фотоапаратах багатьох фірм, в тому числі "Canon" і "Fuji". Вбудовані програми пошуку можуть автоматично знаходити в зображенні видошукача людські обличчя за характерними ознаками – очами, вухами, носом і т.д. Фірма "Sony" розробила цифрову камеру, яка утримує затвор від спрацьовування до тих пір, поки люди не посміхнуться, досліджуючи положення куточків рота, розмикання губ, мімічні зморшки навколо очей. Розробляються програми для розпізнавання обличчя за допомогою камер мобільних пристроїв. Смартфони Apple реалізують цю функцію.

Компанії, які є лідерами в розробці технологій розпізнавання обличчя: ZN Vision Technologies (системи ZN-Face, ZN-Phantomas і ZN SmartEye), SAFLINK (біометричні add-on-модулі для Windows), Imagis Technologies (CABS – інтегрована система обліку правопорушень і злочинців). Також на ринку представлені компанії Geometrix (3D сканери обличчя), Genex Technologies (3D сканери обличчя) в США, Cognitec Systems GmbH (SDK, спеціальні обчислювачі, 2D камери) в Німеччині, Bioscrypt (3D сканери обличчя).

Висновки

1. Серед біометричних методів, які стали вже традиційними, найбільш перспективним є розпізнавання людини по обличчю. Цей метод має ряд незаперечних переваг перед більшістю інших: при досить високій точності визначення він дозволяє проводити перевірку на відстані, допускає таємну перевірку і вимагає наявності тільки відеокамери. Розроблено досить велике число алгоритмів, що забезпечують не тільки високу швидкодію і точність визначення, але і дозволяють системі працювати в самих різних умовах. Сукупність цих якостей зумовила дуже швидкий розвиток цього методу, поставивши його за поширеністю в один ряд з дактилоскопічної перевіркою.

2. Для підвищення точності необхідно об'єднання кількох різних алгоритмів, які аналізують обличчя. Наприклад, доповнюють розпізнавання обличчя розпізнаванням особи по вушній раковині, яка забезпечує високий відсоток збігу. Варто відзначити, що не завжди доцільно використовувати велику кількість алгоритмів, так як приріст ймовірності розпізнавання може бути не суттєвий.

3. Однією з найбільш перспективних тенденцій розвитку ринку біометрії є поява інтелектуальних цифрових відеокамер, що реалізують функцію виявлення обличчя на основі вбудованої логіки. Інтелектуальні відеокамери дозволяють отримувати не тільки якісний відеопотік, а й пов'язані з ним метадані, що містять відомості про знайдені обличчя. Такий підхід дозволяє значно знизити навантаження на апаратні потужності системи розпізнавання, що, в свою чергу, зменшує кінцеву вартість біометричних комплексів, роблячи їх більш доступними для кінцевого споживача. Крім того, зменшуються вимоги до

каналів передачі даних, оскільки при такому підході досить наявності стандартних мереж для передачі стисненого відео і незначного потоку детектованих зображень облич.

4. Сучасні системи розпізнавання особи по обличчю знаходять застосування не тільки для серйозних завдань типу виявлення розшукуваних осіб в місцях масового перебування людей, а й для суто цивільних цілей. Через широке поширення недорогих веб-камер і розробки нових алгоритмів розпізнання обличчя, що дозволили істотно підвищити точність методу, контроль доступу до персональних комп'ютерів по обличчю користувача стає все більш значущим сегментом ринку біометричних технологій. Аналіз найпоширеніших програм показує, що вони мають досить малу ймовірність помилок, забезпечують зручність в роботі. Їх характеристики приблизно однакові і вибір залежить від особистих вимог користувача.

5. Ефективно розпізнавати обличчя можна тільки в певних умовах, саме тому вкрай важливо при впровадженні біометрії обличчя розуміти, в яких умовах буде експлуатуватися система. Однак для більшості сучасних систем розпізнавання ці умови цілком досяжні на реальних об'єктах. Так, для підвищення ефективності розпізнавання обличчя в ідентифікаційних зонах слід організовувати спрямований потік людей для забезпечення можливості короткочасної фіксації обличчя кожного відвідувача. При цьому камери відеофіксації повинні бути встановлені з такою умовою, щоб кут відхилення зафіксованих облич від фронтального положення не перевищував 20–30 град.

Дотримання цих умов при впровадженні систем розпізнавання дозволяє ефективно вирішувати завдання ідентифікації особи і пошуку людей, що представляють певний інтерес, з ймовірністю, максимально наближеною до декларованих розробниками значень показників успішної ідентифікації.

Література

1. Бугаєнко Х.А. Аналіз трьох біометричних методів автентифікації особи [Електронний ресурс] / Х.А. Бугаєнко, І.Д. Горбенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 262–266. – Режим доступу : http://nbuv.gov.ua/UJRN/Prre_2012_11_2_27.

2. Концепція створення національної системи ідентифікації громадян України, іноземців та осіб без громадянства [Електронний ресурс] : розпорядження КМУ від 23 грудня 2015 р. № 1428-р. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/1428-2015-%D1%80.

3. Хрулев А. Системы распознавания лиц. Состояние рынка. Перспективы развития [Електронний ресурс] / А. Хрулев // Системы безопасности. – 2012. – № 1. – С. 70–72. – Режим доступу : http://secuteck.ru/articles2/videonabl/sistemi-raspoznavaniya-lic.

4. Корпань Я.В. Аналіз методів та алгоритмів компресії-декомпресії цифрових відеоданих / Я.В. Корпань // Вісник Хмельницького національного університету. – 2015. – № 3. – С. 175–179.

5. Корпань Я.В. Методи та алгоритми компактного представлення графічної інформації в комп'ютерних системах / Я.В. Корпань // Технологічний аудит та резерви виробництва. – 2015. – Т. 3, № 2 (23). – С. 32–36. – doi: 10.15587/2312-8372.2015.43330.

6. Лысак А.Б. Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем / А.Б. Лысак // Математические структуры и моделирование. – 2012. – № 2(26). – С. 124–134.

7. Татарченко Н.В. Биометрическая идентификация в интегрированных системах безопасности [Электронный ресурс] / Н.В. Татарченко, С.В. Тимошенко // Специальная техника. – 2002. – № 2. – Режим доступа : http://www.ess.ru/sites/default/files/files/articles/2002/02/2002_02_03.pdf.

8. Savvides M. Face Verification using Correlation Filters / Marios Savvides, B.V.K. Vijaya Kumar, Pradeep Khosla // Electrical and Computer Eng. Dept, Carnegie Mellon University Pittsburgh, U.S.A. URL: http://www.ece.cmu.edu/~kumar/Biometrics_AutoID.pdf.

9. Marcel S. On the recent use of local binary patterns for face authentication / Sebastien Marcel, Yann Rodriguez, Guillaume Heusch // International journal of image and video processing, Special issue on facial image processing. URL: http://www.idiap.ch/~marcel/professional/publications/marcel-ijivp-2007.pdf.

10. Моржаков В. Современные биометрические методы идентификации [Электронный ресурс] / В. Моржаков, А. Мальцев // БДИ. – 2009. – № 2. – Режим доступа : http://habrahabr.ru/blogs/infosecurity/126144/.

Рецензія/Peer review : 29.6.2016 р. Надрукована/Printed : 25.8.2016 р.
Рецензент: д.т.н., проф., В.М. Рудницький