МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

Кафедра комп'ютеризованих систем управління

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____Литвиненко О.Є.

«___» _____2020 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"

Тема: Система ідентифікації особи за біометричними даними

Виконавець: Халітов Є.В.

Керівник: Нечипорук В.В.

Нормоконтролер: Тупота Є.В.

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютеризованих систем управління
Освітнього ступеня магістр
Спеціальність 123 "Комп'ютерна інженерія"
(шифр, найменування)
Спеціалізація 123.02 "Системне програмування"
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Литвиненко О. Є.

«____»_____2020 р.

ЗАВДАННЯ
на виконання дипломної роботи (проекту)

Халітов Євгеній Валерійович
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема роботи: "Система ідентифікації особи за біометричними даними"

затверджена наказом ректора від "07" вересня 2020 року № 1410 /ст.
2. Термін виконання роботи: з 05.10.2020 до 31.12.2020
3. Вихідні дані до роботи: 1) вимоги до змісту системи;
2) основні функції системи
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1) аналіз біометричних систем ідентифікації особистості;
2) використання апаратних та програмних засобів ідентифікації особистості за біометричними параметрами;
3) розробка програмної системи ідентифікації особистості через розпізнавання графічних та аудіо файлів.
5. Перелік обов'язкового графічного матеріалу:
1) методи ідентифікації на основі аналізу характерних точок і відстаней;
2) приклад кластеризації кодового словника аудіозаписів;
3) компоненти бібліотеки *OpenCV*;
4) зв'язки модулів програми;
5) вікно системи ідентифікації особи за зображенням;
6) схема алгоритму перетворення графічної інформації до двійкової.

ц

6. Календарний план

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1	Провести аналіз літератури за темою дипломної роботи та аналіз існуючих систем	05.10.2020 – 06.10.2020	
2	Підготувати перший розділ пояснювальної записки	07.10.2020 – 10.11.2020	
3	Розробити структуру програмної системи	11.11.2020 – 14.11.2020	
4	Розробити програмні засоби. Підготувати другий розділ пояснювальної записки	15.11.2020 – 19.11.2020	
5	Провести налаштування та тестування системи	20.11.2020 – 03.12.2020	
6	Завершити оформлення пояснювальної записки	04.12.2020 – 13.12.2020	
7	Підготувати презентацію та графічні матеріали	14.12.2020 – 22.12.2020	

7. Дата видачі завдання 05.10.2020

Керівник Нечипорук В.В.
(підпис)

Завдання прийняв до виконання Халітов Є.В.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи “Система ідентифікації особи за біометричними даними”: 86 с., 15 рис., 24 літературних джерела, 1 додаток.

РОЗПІЗНАВАННЯ ОБРАЗІВ, НЕЙРОННІ МЕРЕЖІ, АЛГОРИТМИ РОЗПІЗНАВАННЯ ОБРАЗІВ, ОБ’ЄКТ ІДЕНТИФІКАЦІЇ, ГРАФІЧНІ ЗОБРАЖЕННЯ

Мета дипломної роботи – ідентифікації особи за рахунок застосування нейромережевої технології розпізнавання графічних зображень та аудіофайлів.

Об’єкт дослідження – ідентифікація особи.

Предмет дослідження – система ідентифікації особи за біометричними даними.

Розроблена в даній роботі програмна система дозволяє ідентифікувати осіб за записом відео, який розділено на аудіо та відео складові.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

GUI – *Graphical User Interface* (графічний інтерфейс користувача)

IDE – *Integrated Development Environment* (інтегроване середовище розробки);

VCL – *Visual Component Library* (бібліотека візуальних компонентів)

FAR – *False Acceptance Rate*

FRR – *False Rejection Rate*

FMR – *False Match Rate*

FNMR – *False Non-Match Rate*

НМ – нейронна мережа.

ВСТУП

У наш час паролі, персональні ідентифікаційні номери і спеціальні ідентифікаційні картки стали життєвою необхідністю. Наприклад, щоб отримати готівку з банкомату, Вам потрібно код *PIN*, щоб отримати доступ до поштовій програмі або до певної категорії комп'ютерних даних, необхідний пароль. У світлі останніх подій, що відбуваються в світі, особливо в зв'язку з ростом активності міжнародного тероризму, питанням безпеки приділяється все більше уваги.

Таким чином, людина повинна зберігати в своїй пам'яті безліч різних комбінацій цифр і букв. Щоб полегшити долю сучасної людини, компанії, що спеціалізуються на виробництві комп'ютерів, почали займатися розробкою біометричних технологій. Біометрія – ця наука, що вивчає можливості використання різних характеристик людського тіла (будь то відбитки пальців або унікальні властивості людського зіниці або голосу) для ідентифікації кожної конкретної людини. Користуючись біометричними технологіями, людина ніколи не зможе забути необхідний йому пароль або код, оскільки його великий палець, голос або зіницю ока завжди знаходяться з ним.

Примусити комп'ютер бачити – завдання не нове і природним чином вписується в концепцію штучного інтелекту. Головне тут – алгоритми обробки зображення, як статичного, так і рухомого.

Одним з самих послідовних і вірних прихильників даного напряму є сфера безпеки. Адже система безпеки – не стільки «глуха огорожа», скільки надійний комплекс заходів по профілактиці і виявленню порушень. Саме тому потенційні користувачі систем безпеки і, звичайно ж, виробники охоронних комплексів зацікавлені в ефективній технології розпізнавання осіб, яка заснована саме на алгоритмах обробки зображення.

Суть цієї технології полягає в тому, що система безпеки автоматично, без участі людини, визначає, що в кадрі знаходиться обличчя людини, а також встановлює, кому саме належить ця особа. Складність цього завдання, проте,

настільки велика, що до цих пір висловлюються великі сумніви в тому, що таку технологію коли-небудь вдасться зробити такою, що працює достовірно. Проте, розробники прикладають багато сил для вдосконалення систем розпізнавання осіб. Чи є ця тема виключно научно-исследовательской, свого роду змаганням, вправою для розуму і інтелекту, або все-таки переслідує практичні цілі? Наскільки подібна система затребувана і застосовна на ринку безпеки?

Щоб відповісти на поставлені питання, слід задатися ще одним: «Для чого потрібне розпізнавання осіб і де воно може використовуватися?». Відповідь проста: скрізь, де необхідно забезпечувати безпеку – на прохідній підприємства, в метро, в аеропорту і на вокзалі, в супермаркеті і на автозаправці, в концертних залах і на стадіонах, на вулицях і площах, в розважальних закладах, в кафе, клубах і ресторанах. Одним словом, скрізь, де можна зіткнутися з «злою волею» і «нечистими намірами» людини. Місія системи розпізнавання осіб в тому і полягає, щоб захистити громадян від посягання на їх права, майно і життя.

Компанія *Google*, коментуючи покупку компанії *Neven Vision* та її оригінальних біометричних розробок, пояснила, що бачить привабливі перспективи інтеграції подібних технологій в свої сервіси для роботи з графічною інформацією, на зразок *Picasa* і *Picasa Web Albums*. Ефективне розпізнавання осіб 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 осіб, програма *Reuters* індексує відеоматеріали агентства, так що найближчим часом користувачі отримають можливість шукати відеосюжети, які містять конкретних людей.

Найпростіші функції розпізнавання осіб вже реалізовані в цифрових фотоапаратах багатьох фірм, в тому числі *Canon*, *Pentax* і *Fuji*. Вбудовані програми пошуку можуть автоматично знаходити в зображенні видошукача людські обличчя за характерними ознаками – очам, вухам, носі і т.д. Якщо особа одне, камера сама може налаштувати фокус виключно на нього, якщо ж осіб кілька, то може обчислити усереднений фокус для всіх. Або, скажімо, лише для

осіб переднього плану. А недавно фірма *Sony* оголосила ще про одну новинку – цифрову камеру, яка утримує затвор від спрацьовування до тих пір, поки люди не посміхнуться, досліджуючи положення куточків рота, розмикання губ, мімічні зморшки навколо очей.

Активно йдуть розробки програм для розпізнавання особи за допомогою камер мобільних пристроїв. Смартфони *Apple* вже реалізують цю функцію.

ZN Vision Technologies (*http://www.zn-ag.com*) – одна з провідних компаній в області автоматичного спостереження і визнаний технологічний лідер в розробці систем безпеки. Рішення базуються на математичних методах, властивих людині (алгоритми нечіткої логіки). Використовуючи патентований метод розпізнавання людини за рисами обличчя, компанія створює продукти для охорони будівель, для пошуку людей в фотоархівах і для «розумного» відеоспостереження. Грунтуючись на технології моніторингу, *ZN Vision Technologies AG* пропонує системи *ZN-Face*, *ZN-Phantomas* і *ZN SmartEye*, що виступають як основні складові для контролю доступу та аналітичного відеоспостереження, ідентифікації і верифікації людей.

Біометричні технології – найбільш надійне і комплексне з наявних рішень по аутентифікації користувачів. Багато в чому саме підвищенням вимог до підсистем аутентифікації, що входять в сучасні системи безпеки, і обумовлено поширення біометричних систем. Системи суворої аутентифікації, як правило, використовують два і більше фактори при аутентифікації користувачів. Наявні системи аутентифікації, побудовані на факторах «*you know*» і «*you have*» надають великі можливості для посилення захисту і можуть бути доповнені біометричними підсистемами. Комбінування традиційних і біометричних засобів дозволяє забезпечити необхідну надійність аутентифікації навіть при використанні біометричних чинників, які самі по собі не є в даний час досить надійними. В першу чергу це справедливо для аутентифікації по геометрії особи. Так, якщо аутентифікація по обличчю сама по собі все ж ще не є в даний час достатньо надійною (особливо з точки зору роботи в умовах різної освітленості), то разом з використанням пароля або карти доступу забезпечує точність

аутентифікації практично достатню навіть для об’єктів з високим ступенем захисту.

Мета дипломної роботи – ідентифікації особи за рахунок застосування нейромережевої технології розпізнавання графічних зображень та аудіофайлів.

Об’єкт дослідження – ідентифікація особи.

Предмет дослідження – система ідентифікації особи за біометричними даними.

Розроблена в даній роботі програмна система дозволяє ідентифікувати осіб за записом відео, який розділено на аудіо та відео складові.

РОЗДІЛ 1
АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ

Хоча до теперішнього часу виявлено безліч фізичних рис людини, придатних для встановлення особи, широкомасштабне їх використання тривалий час стримувалося відсутністю апаратних і програмних засобів, що дозволяють автоматизувати процес біометричної ідентифікації. Поява останнім часом нових технологій, що вирішують цю задачу, і їх стрімке здешевлення, зробили широко доступними біометричні системи ідентифікації, які раніше використовувалися тільки вузьким колом особливо уповноважених осіб.

В даному розділі при аналізі сучасного стану в області біометричних технологій використовується термін «ідентифікація», як складова частина сталого виразу «*biometric identification*», що описує біометричну перевірку в широкому сенсі слова, включаючи також і аутентифікацію.

1.1. Загальні відомості щодо біометричних технологій

У всіх біометричних технологіях існує очевидний загальний підхід до вирішення завдання ідентифікації – кожна біометрична технологія передбачає поетапне виконання наступної послідовності дій:

– сканування суб’єкта ідентифікації (один або декілька вимірів біометричної характеристики зі зчитувального пристрою);

– перетворення отриманих про суб’єкта даних в придатну для використання цифрову форму, витяг індивідуальної інформації;

– формування за заданим алгоритмом індивідуального ідентифікатора для даного суб’єкта;

– порівняння поточного ідентифікатора з базою даних (або з даними всіх користувачів, або тільки певного, в разі наявності додаткової інформації про суб’єкта) [7].

Хоча розроблені розпізнавальні методи біометричної ідентифікації досить різноманітні, принципово все вони можуть бути розділені на дві великі групи:

– статичні методи – засновані на аналізі будь-якої фізіологічної характеристики людини, унікальною для кожного, властивою йому від народження і невід'ємною від нього;

– динамічні методи – аналізують поведінкові характеристики людини, особливості підсвідомих рухів в процесі відтворення якого-небудь дії (підписи, мови, клавіатурного набору).

Певні фізіологічні особливості людини, такі, як папілярний узор пальця, геометрія особи, температура шкіри обличчя, форма вуха, малюнок вен руки, геометрія долоні, малюнок райдужної оболонки ока або сітківка ока, структура ДНК, є постійними і незмінними протягом усього життя фізичними характеристиками людини. Як і самі ці фізіологічні характеристики, вимірювання статичного типу дають практично незмінний для кожної людини результат. Оскільки людина сама є ключем, ці методи перевірки відрізняються зручністю застосування і точністю результатів.

Загальновідомо також, що кожна людина має деякі індивідуальні поведінкові характеристики, за якими можна його ідентифікувати: особливості підпису, голос, рукописний або клавіатурний почерк, хода. На відміну від фізіологічних особливостей, вони можуть змінюватися з плином часу, тому зареєстрований біометричний зразок повинен оновлюватися при кожному його використанні. Крім того, поведінкові риси є керованими і знаходяться під впливом не тільки свідомих дій людини, але і некерованих психологічних факторів (настрій, стан здоров'я, стрес), що може значно знизити точність ідентифікації. Тому хоча біометрія, заснована на поведінкових характеристиках, менш дорога і представляє меншу загрозу для конфіденційності біометричних даних користувачів,

Деякі методи біометричної ідентифікації, які отримали найбільш широке поширення, розглянуті нижче [8, 10].

1.1.1 Розпізнавання за відбитками пальців

В основі цього методу біометричної ідентифікації лежить унікальність малюнка папілярних візерунків на пальцях кожної людини. Переваги – простота використання, швидкість і надійність. Соціологічні дослідження також показали, що використання відбитка пальця є найзручнішим для користувачів біометричних методом. Крім того, біометричний сканер відбитка пальця досить компактний і вміщується навіть на клавіатурі.

Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетвориться в цифровий код (згортку) і порівнюється з раніше введеним еталоном. Існує два основних алгоритму порівняння отриманого коду з наявними в базі шаблоном: по характерних точках і по всій поверхні пальця. У першому випадку виявляються характерні ділянки і їх взаємне розташування. У другому випадку запам’ятовується весь відбиток. Іноді використовується також комбінація алгоритмів, що дозволяє підвищити надійність системи.

Зазвичай в базі даних зберігають кілька еталонних образів, що дозволяє підвищити точність ідентифікації. Вони можуть відрізнятися зрушенням і поворотом, максимальний кут повороту відбитка від вертикалі не більше 15 градусів [4].

В середньому відсоток негативної ідентифікації легальних користувачів становить близько 3%, а відсоток помилкової позитивної реакції – менше одного до мільйона. Така ймовірність помилки набагато менше в порівнянні з іншими біометричними методами, особливо якщо врахувати, що середня імовірність розпізнавання відбитків пальців криміналістом дорівнює приблизно 70%, хоча дактилоскопія використовується понад 100 років і вважається досить надійною [9].

1.1.2. Розпізнавання за формою кисті руки

Цей порівняно новий статичний метод, який викорстовувався у криміналістиці, виконує ідентифікацію по скануванню руки. В даних біометричних системах використовується геометрична форма кисті руки (або

декількох пальців), а попутно – розташування підшкірних кровоносних судин долоні, візерунок ліній на долоні. При цьому мова може йти про різні методи.

Ідентифікація по геометрії руки за своєю технологічною структурою та рівнем надійності порівняння з методом дактилоскопічної ідентифікації. Найчастіше ці методи використовуються спільно, хоча пристрій для зчитування відбитків долонь займає більше місця. Вимірювання для отримання унікальної цифрової згортки виробляються за допомогою спеціального пристрою, що дозволяє отримувати тривимірний образ пензля руки (або, за допомогою відеокамери, знімки і внутрішньої, і збоку долоні).

Однак форма кисті руки досить сильно змінюється з часом.

1.1.3. Розпізнавання за райдужною оболонкою ока

При цьому розпізнаванні проводиться вимір і аналіз кольорового кільця навколо зіниці. Факт відсутності двох осіб з однаковою райдужною оболонкою ока (більше того, навіть у однієї людини райдужні оболонки очей відрізняються один від одного) був доведений ще в 1950-х роках. Однак технічна реалізація методу розпізнавання по райдужній оболонці ока з'явилася відносно недавно – патент на цю технологію було отримано в 1994 році. Унікальність даної технології полягає в тому, що в райдужці зберігається більше інформації, ніж в будь-якому іншому органі людського тіла (266 унікальних точок ідентифікації в порівнянні з 10-60 точками у інших методів).

Не потрібно спеціальних умов, наприклад, щоб користувач зосередився на цілі, тому що райдужна оболонка знаходиться на поверхні ока. Порушення зору і пошкодження кришталика ока (катаракта) ніяк не впливає на точність сканування. Патентований код, прийнятий у всіх комерційних системах ідентифікації, гарантує частоту помилок близько 1 на 1,2 мільйона. Існуючі рішення дозволяють ідентифікувати користувача навіть при затіненні (або пошкодженні) райдужної оболонки по 1/3 зображення райдужної оболонки з ймовірністю помилки 1 до 100 тис. Подібну надійність не можуть забезпечити інші біометричні технології.

Для реалізації методу необхідна лише камера, що дозволяє отримати зображення з достатнім дозволом, і спеціалізоване програмне забезпечення, що дозволяє виділити з отриманого зображення малюнок райдужної оболонки ока, за яким будується цифровий код для ідентифікації людини. Фактично, сучасними камерами очей може бути відсканований на відстані метра, що розширює можливості використання методу [6].

1.1.4. Розпізнавання за сітківкою ока

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судинах на задній стінці ока. Зображення райдужної оболонки має бути чітким, тому катаракта може негативно впливати на якість ідентифікації особистості.

Сканери сітківки набули широкого поширення в системах контролю доступу на особливо секретні об’єкти, так як у них один з найнижчих відсотків відмови в доступі легальних користувачів і практично не буває помилкового дозволу доступу.

Незважаючи на схожість і майже однакову надійність, даний метод не є парним зі скануванням райдужної оболонки, так як використовуються різні сенсори, з різними вимогами до одержуваному образу.

1.1.5 Розпізнавання за формою обличчя

Це самий інтуїтивно зрозумілий метод ідентифікації, найбільш близький людині. В даному статичному методі ідентифікації будується образ особи, а на ньому виділяються індивідуальні параметри. Кількість, якість і різноманітність (різні кути повороту голови, зміни нижньої частини обличчя при вимові ключового слова і т.д.) зчитувальних образів може варіюватися в залежності від алгоритмів і функцій системи, що реалізує даний метод.

Ідентифікація за рисами обличчя – одне з найбільш динамічно розвиваються, у біометричної індустрії, однак більшість розробників поки зазнають труднощів в досягненні високого ступеня надійності систем.

1.1.6 Розпізнавання по рукописному почерку (за підписом)

Як правило, для цього динамічного методу ідентифікації використовується написання кодового слова або підпис людини. Цифровий код ідентифікації формується за динамічними характеристиками написання, тобто по графічним параметрам написи, тимчасовим характеристикам написання і динаміки натиску на поверхню в залежності від можливостей обладнання (планшет, екран кишенькового комп'ютера і т.д.).

Для ідентифікації підпису використовують спеціальні ручки, чутливі до тиску панелі, або комбінацію обох. Пристрої зі спеціальними ручками менш дороги і займають менше місця, але в той же час мають менший термін служби.

1.1.7 Розпізнавання за голосом

Голос індивідуальний для кожної людини і формується з комбінації фізіологічних і поведінкових факторів. Існує досить багато способів побудови коду ідентифікації по голосу: як правило, це різні поєднання частотних і статистичних характеристик голосу.

Біометричний підхід, пов'язаний з ідентифікацією голосу, є однією з найстаріших технологій і, в той же час, вкрай зручний в застосуванні. Головним його недоліком є низька точність ідентифікації через високу залежність від нефіксованих зовнішніх факторів (наприклад, захворювання горла). Розпізнавання по голосу має точність, порівнянну з гіршими статичними алгоритмами, але і то лише в ідеальних умовах. Необхідно відзначити, що інші динамічні методи ще менш надійні. Хоча ідентифікація особистості по голосу не так надійна, як багато інших біометричні методи, це стає все менш серйозною проблемою в міру того, як пристрої голосового ідентифікації розрізняють нові додаткові характеристики людської мови [8].

Існує також багато інших маловідомих напрямків в області біометрії, як уже невикористовуваних, так і перспективних, які зараз слід визнати швидше екзотичними. Наприклад, розпізнавання по вушній раковині, термограмме особи, по серцевому ритму, аналізу фрагментів ДНК, запаху і т.п. Більшість цих

технологій знаходиться ще на стадії досліджень і зараз їх частка на ринку і вплив на розвиток біометрії невисокі.

Кожен з параметрів має свої переваги і недоліки з точки зору його використання в якості критерію ідентифікації. Останнім часом ведуться активні розробки з удосконалення та модифікації систем ідентифікації особистості, пошук нових підходів для характеристики людської індивідуальності, комбінації фізіологічних і поведінкових факторів.

1.2. Аналіз ринку біометричних систем розпізнавання особистості

Як і в інших галузях, для вивчення стану світового ринку біометричних технологій необхідно проводити цілий комплекс масштабних статистичних та аналітичних досліджень, опитувань споживачів і виробників. Існують спеціалізуються на цьому науково-технічні та аналітичні організації, які спостерігають за функціонуванням ринку і оцінюють його розвиток. Скористаємося даними, наданими деякими з таких організацій, для аналізу сучасного стану на ринку засобів біометричної ідентифікації. Однак необхідно мати на увазі, що в різних джерелах подібні дані коливаються в межах 15-20%, так що це всього лише оціночне уявлення.

1.2.1. Розвиток та сучасний стан світового ринку

Перші біометричні системи спочатку набули поширення як системи підвищеної безпеки, так як дозволяли забезпечити небувалу тоді ступінь захисту від несанкціонованого доступу. Це було обумовлено не тільки власними перевагами біометричного підходу, але і його новизною. Висока вартість перших систем обмежувала сферу їх застосування в основному засекреченими державними об’єктами.

Доступні за ціною мікропроцесорні системи біометричного контролю для приватного бізнесу з’явилися на початку 1990-х років. Стрімке здешевлення в останні роки електронного устаткування і поява нових технологій (особливо розробка недорогих мікропроцесорів і техніки для роботи з зображенням)

дозволило значно розширити перелік об’єктів, що захищаються і збільшити точність біометричних пристроїв [7].

В Україні біометричні системи контролю з’явилися в середині 1990-х років. Через нерозвиненість власних технологій (або їх зайвої засекреченість) все комерційні біометричні системи були імпортного виробництва. Ціна цих систем була досить висока: наприклад, досить простий пристрій фізичного контролю доступу коштувало близько 12 000 $ [6]. Подібне дороге устаткування мало характер новомодної екзотики і масового поширення не одержало.

Різке підвищення ролі біометричних технологій відбулося після подій в США 9 вересня 2001 р вельми наочно підтвердили необхідність широкого застосування систем, здатних ідентифікувати окремих осіб в місцях скупчення людей. З того моменту біометричні системи безпеки все помітніше виступають на лідируючі позиції в індустрії безпеки, в боротьбі зі злочинністю та тероризмом. Їх значення в комплексному забезпеченні безпеки неухильно зростає, що особливо яскраво проявляється на прикладах систем безпеки в аеропортах та інших важливих інфраструктурних об’єктах.

Розвиток біометричних технологій також стимулюється повсюдним усвідомленням того факту, що інші способи ідентифікації (по паролів, фотографій, ПІН-кодами) вельми обмежені в своїх можливостях і стають все більш уразливими для організованої злочинності і небезпечними. Повсюдне прагнення організувати сучасну, грамотно побудовану систему безпеки на підприємстві, в офісі компанії або в приватному будинку ведуть до того, що замовники роблять вибір на користь біометрії.

Сьогодні, як і в усьому світі, так і в Україні, біометричні системи стали набагато дешевше (більш ніж в 10 разів), що стало економічною причиною появи активного попиту на них серед найширшого кола споживачів, аж до рядових громадян. Можна навести безліч прикладів успішної роботи пристроїв, побудованих на біометричний принципі. Станом на 2018 рік доступ вже більш ніж в 10 тис. об’єктів (комп’ютеризованих місць, сховищ, дослідницьких лабораторій, банків крові, банкоматів, військових споруд) контролювався біометричними пристроями за фізіологічними або поведінковими

характеристиками індивідуума [7]. Є і суто цивільні об'єкти: в США використовуються банкомати, що розпізнають клієнтів в обличчя і, упізнавши їх, вітають по імені; увійти в Діснейленд можна,

Розглядаючи практично будь-які дані, легко помітити повсюдний прогресуючий зростання показників ринку біометрії.

Обсяг продажів на ринку біометричних технологій в США в 1999 році становив 58,4 млн. $ (*International Data Corp.*), але вже до 2000 року перевершив рубіж в 100 млн. $, Що було обумовлено широкомасштабним впровадженням біометричних технологій в повсякденне життя.

У 2002 році доходи світової біометричної індустрії становили 600 млн. $, в 2009 році – 4,2 млрд. $ (*Frost* & *Sullivan*), а в 2012 р – вже 7,56 млрд. $ (*Biometrics Research Group*).

Близько половини цього ринку становлять рішення для «цивільного» сектора, що застосовуються в торгових компаніях, банках, держсекторі і освітніх установах. Причому це не тільки системи безпеки, а й, наприклад, рішення для моніторингу робочого часу співробітників.

Найбільший сегмент біометричного ринку стійко формують дактилоскопічні системи: в 2018 р. на частку цього сегмента доводилося 5 млрд. $, і очікується, що до 2021 р цей показник досягне 10 млрд. $.

Найбільшим регіональним ринком в розглянутому сегменті були і залишаться США (*GIA*). Що ж стосується швидкості розвитку технологій біометричної ідентифікації, то тут найбільш високі результати демонструють країни Азіатсько-Тихоокеанського регіону (АТР): у 2019 р. обсяг біометричного ринку в країнах Азійсько-Тихоокеанського регіону (АТР) склав близько 500 млн. $, І в найближчі п'ять років середньорічні темпи його зростання, обчислені в складних відсотках, досягнутий 12,6% (*Frost* & *Sullivan*). Причому розпізнавання по обличчю і голосу середньорічні темпи зростання, обчислені в складних відсотках (*CAGR*), досягнутий тут 28,5%.

Це обумовлено тим, що для країн АТР пріоритетним завданням зараз є формування інфраструктури систем національної ідентифікації та прикордонного контролю. Роль технологій біометрії тут настільки велика, що біометричний

ринок в АТР буде розвиватися швидше, ніж в Північній Америці, на Середньому Сході і в європейських державах. Найбільш яскравою рисою становлення біометричного ринку в АТР стало формування систем національних ідентифікаційних карт, що містять біометричні дані власників (перш за все про відбитки пальців). Ці *ID*-карти допомагають урядовим органам країн АТР ефективно ідентифікувати добропорядних громадян і протидіяти діяльності повстанських угруповань.

В Україні також особливо широкого поширення набули дактилоскопічні пристрої, попит на які останнім часом різко зріс з боку приватних осіб, які встановлюють їх в заміських котеджах. Великою рідкістю в Україні вважаються системи ідентифікації особи за райдужною оболонкою ока, голосу або за іншими біометричними ознаками (хоча є приклади їх використання в ряді великих депозитарних банків Києва).

У розрізі географії виробників перше місце на українському ринку займають американські та західноєвропейські компанії. Власні українські розробки відрізняються крайньою фрагментарностью, існують на рівні дослідних зразків і говорити про скільки-небудь серйозних обсягах їх продажів, поки не доводиться. В основному ринок біометричних систем безпеки в Україні представлений іноземними фірмами, які через українських партнерів реалізують свої технології.

1.2.2. Технології дактилоскопічної ідентифікації

Згідно зі світовою статистикою, технології, засновані на обробці відбитків пальців, займають лідируюче положення з величезним відривом, по ряду оцінок – до 52% від загального числа біометричних рішень. Не тільки за кордоном, але і в Україні домінують рішення, що ідентифікують користувачів по відбитках пальців, займаючи більше половини обсягу отраслевого ринку.

На додаток до інших засобів безпеки, пристрої доступу по відбитку пальців встановлені у військових установах США, включаючи Пентагон і урядові лабораторії. Дана технологія набула великого поширення в системі автоматичної

ідентифікації по відбитку пальця (*AFIS*), використовуваної поліцією в США і в більш ніж 30 країнах. Сумарний дохід виробників в 2019 році склав 462 млн. $

Існує кілька причин такого стану речей. Технологія ідентифікації і верифікації за відбитками пальців має досить глибоке історичне коріння і, як наслідок, потужну теоретичну і практичну базу (наприклад, правоохоронними відомствами накопичені дуже великі бази даних про відбитки пальців). Крім того, постійно удосконалюються процеси сканування та обробки зображень, покращуючи і без того непогані характеристики надійності. Поява широкого асортименту ефективних і досить дешевих коштів по обробці відбитків пальців забезпечує високу надійність при такій дешевизні рішень «під ключ», що навіть пересічні громадяни встановлюють дактилоскопічні сканери в приватних будинках.

У сегменті обліку робочого часу та контролю доступу ця тенденція проявляється особливо зримо: в масових масштабах і виробляються, і закуповуються саме дактилоскопічні системи, тоді як, скажімо, розпізнавання по малюнку вен або геометрію кисті руки виглядає екзотично.

Існує досить багато компаній, які займаються технологіями контролю доступу по відбитку пальців, хоча лідируючі позиції традиційно займають американські компанії.

Незважаючи на велику кількість фірм, які займаються даною тематикою, близько 80% всіх дактилоскопічних систем у всьому світі доводиться на одну компанію – *Identix* (*http*://*www.identix.com*/).

1.2.3. Розпізнавання за формою обличчя

Друге за величиною місце на ринку систем біометрії займає напрямок, пов’язаний з технологіями розпізнавання особи. В останні роки темпи зростання цього сегмента різко зросли, і ідентифікація по обличчю з кожним роком займає все більш високі позиції в рейтингах.

Такий стрибок пояснюється разючою вдосконаленням відеообладнання і алгоритмів їх обробки (в тому числі і якість стиснення компресорами –

кодеками). Тоді як спочатку розпізнавання особи мало неприйнятно низьку надійність, нові можливості цифрового відео вивели його на якісно новий рівень.

Поряд з цим, свою роль зіграло і те, що тут не потрібно великих інвестицій в інфраструктуру, дозволяючи використовувати вже наявні кошти (системи відеоспостереження), що особливо привабливо для державних і правоохоронних органів. Також важливо, що ця технологія пасивна, тобто не вимагає прямого контакту з суб'єктом ідентифікації і допускає потайливу ідентифікацію, що також дуже затребуване в поліцейських цілях.

Як приклад діючої системи контролю доступу на базі розпізнавання обличчя можна привести систему розпізнавання відвідувачів місць для переведення в готівку чеків, встановлених компанією *Mr. Payroll* в декількох штатах США. Широко відома і система *Facelt*, що працює на вулицях англійського міста Ньюхем, а також в аеропортах, стадіонах і торгових центрах США.

Загальносвітовий показник середньорічного темпу зростання, виражений в складних відсотках (*CAGR*), для сегмента технологій ідентифікації по обличчю – 19% (*Frost & Sullivan*).

Найбільшим регіональним ринком в розглянутому сегменті були і залишаються США (*GIA*). Однак найбільшу швидкість розвитку біометричної ідентифікації по голосу і обличчю демонструють країни Азіатсько-Тихоокеанського регіону, де *CAGR* досягла небувалої величини 28,5%.

Провідні виробники в області розглянутих технологій: *AcSys Biometrics* (*http://www.acsysbiometrics.com/*), *A4Vision* (*http://www.a4vision.com/*), *Cognitec Systems* (*http://www.cognitec.com/*), *Identix* (*http://www.identix.com/*), *Imagis* (*http://www.imagistechnologies.com/*), *Vicar Vision* (*http://www.vicarvision.nl/*), *ZN Vision* (*http: / /www.zn-ag.com/*).

1.2.4. Розпізнавання за формою руки

Цей метод, досить поширений ще 10 років тому, останні роки йде на спад. З самого початку очікувалося, що сканування руки займе досить великий сегмент технологічного ринку але, швидше за все, буде об'єднано з яким-небудь іншим

біометричним напрямком, наприклад з аналізом відбитків пальців або розпізнаванням по венах.

В даний напрямок вкладають гроші великі державні охоронно-правові органи деяких провідних світових держав [6]. Станом на 2003 рік в США метод ідентифікації по геометрії руки використовувався більш ніж в 8000 об'єктів, включаючи Колумбійський законодавчий орган, міжнародний аеропорт Сан-Франциско, лікарні і імміграційні служби.

Пристрої, які можуть сканувати і інші параметри руки, розробляються декількома компаніями: *BioMet Partners* (*http://www.biomet.ch/*), *Recognition Systems* (*http://www.recogsys.com/*), *Palmetrics* і *BTG* [7] .

1.2.5. Розпізнавання за райдужною оболонкою ока

Системи розпізнавання райдужної оболонки ока не тільки найнадійніші, але і найдорожчі. Крім того, їх розробка і передача технології широкому колу розробників і споживачів обмежується строгим патентом (патент США 1994 року фірми *Iridian*). Цими фактами пояснюється порівняно невелика частка подібних систем на ринку [6].

Допуск по райдужній оболонці ока застосовується в державних організаціях США, в тюрмах, в установах з високим ступенем секретності (зокрема, на заводах з виробництва ядерного озброєння).

Найбільший виробник обладнання в цій галузі в даний час – компанія *Iridian* (*http://www.iridiantech.com/*), на рішеннях якій базуються практично всі інші розробки. Крім неї, розробкою займаються понад 20 компаній, в тому числі *British Telecom, Sensar, Saflink, LG, Panasonic, Oki*.

1.2.6. Системи розпізнавання за голосом

Технології розпізнавання голосу – одна з найстаріших біометричних технологій. Останнім часом її розвиток значно прискорилося, так як передбачається широко використовувати голосове управління в інтелектуальних будівлях і в побутовій техніці.

Зараз через недостатню точності ідентифікація по голосу використовується для управління доступом тільки в приміщення низькою і середнього ступеня безпеки, наприклад, лабораторії виробничих компаній.

1.2.7. Розпізнавання по рукописному почерку

Статична закріплення підпису стає вельми популярним, особливо в банківських структурах, де підпис – традиційна, здавна використовується в банківській справі біометрична характеристика. До того ж багато людей набагато більше довіряють звичних способів ідентифікації, серед яких – звичайна підпис.

На світовому електронному ринку пристрої введення рукописних символів вже давно перестали бути екзотикою. І саме тому за останні роки технологія електронного розпізнавання підпису, стає все більш упевненим гравцем на біометричний ринку.

Замість розпису ручкою, для перевірки підпису на банківських кредитних картах, бланках служби доставки *FedEx* вже зараз часто закріплюються біометричні дані. Компанія *CIC* успішно інтегрувала свої рішення на платформу *Pocket PC*.

Втім, фінансове співтовариство не поспішає приймати автоматизовані методи ідентифікації підпису, так як їх все-таки ще занадто легко підробити, що перешкоджає впровадженню ідентифікації за підписом в високотехнологічні системи безпеки.

Провідні виробники: *CIC* (*http*://*www.cic.com*/), *BioPassword Security Software* (*http*://*www.biopassword.com*/), *Checco* (*http*://*www.biochec.com*/).

1.2.8. Прогнози і перспективи розвитку ринку біометричних систем

Альтернативою біометричних систем є системи контролю доступу, реалізовані на базі безконтактних карт або електронних міток *RFID*, однак, біометричні ідентифікатори більш надії, а останнім часом їх вартість стала порівнянна з картами і мітками, що, безсумнівно, забезпечить біометрії більш масове застосування.

Більшість прогнозів зводиться до того, що впровадження біометричних систем безпеки придбає в недалекому майбутньому лавиноподібний характер. Пошук рішень для боротьби з глобальною загрозою тероризму, так чи інакше, приведе до практичного використання досягнень в цій області [7].

Ще одним дуже важливим чинником, що обумовлює зростання потреби в біометричних системах і технологіях, є реалізація масштабних державних проектів по переходу на біометричні паспорти і активне використання біометрії при оформленні віз і в контролі міграційних потоків.

Крім систем безпеки, на думку аналітиків, біометричні технології протягом 2021-2025 рр. будуть активно впроваджуватися в організаціях фінансового сектора, охороні здоров'я та електронної комерції. Основними областями застосування в наступні п'ять років стануть все ж громадянська ідентифікація в невійськових цілях і доступ до комп'ютера (мережі).

Біометричні технології мають значний простором для подальшого розвитку і в великих корпоративних структурах. Біометричні технології здатні посилити корпоративну безпеку, виключивши потреба в численних ідентифікатори, з успіхом замінюються на унікальні для кожного співробітника біометричні характеристики.

Більшість опитаних споживачів визнають контроль фізичного доступу і облік робочого часу найперспективнішою сферою застосування технологій біометрії. Захист офісів і знаходяться в них людей і матеріальних цінностей однаково значима як для великих компаній, так і для невеликих фірм, а заробітна плата співробітників і пов'язані з її нарахуванням платежі входять число найбільш витратних статей в будь-якій організації. У зв'язку з цим будуть затребувані інтегровані системи з біометричними рішеннями, які здійснюють не тільки контроль доступу, але одночасно і облік робочого часу, з кадровою системою і автоматичною передачею результатів для розрахунку заробітної плати. В рамках *HRM*-рішення інтегровані системи проводять оцінку робочого часу відповідно до планового графіком кожного співробітника, дозволяють використовувати отримані дати для розрахунку заробітної плати. Такі, наприклад, проекти в компаніях «Аеромар» і «Кнауф Гіпс Дзержинськ». Серед

найбільш відомих на українському ринку біометричних рішень для обліку робочого часу система «Таймекс» (від «Армо-Системи»), *BioTime* («Біолінк Солюшенс»), *BioSmart* (виробництва «Прософт-Системи»), система «Сонда» (від компанії «Сонда Технолоджи») і *Senesys* (від «Елвіс»).

Ідентифікація особистості по відбитку пальця є безумовним лідером на ринку біометричних рішень і, найімовірніше, буде найбільш широко використовуватися і в майбутньому.

Оскільки практично всі системи контролю доступу оснащуються системами відеоспостереження, то перспективним є системи розпізнавання осіб. В даний час це досить дороге рішення і достовірність реєстрації недостатня. Технології розпізнавання особи, швидше за все, будуть комбінуватися з іншими технологіями для забезпечення більш високих показників надійності, наприклад, може бути перспективно поєднання системи розпізнавання особи з системами інфрачервоної реєстрації.

Відзначається також інтеграція з іншими технологіями, з метою підвищення надійності роботи систем в цілому. Подальше підвищення надійності буде забезпечено включенням відразу декількох біометричних технологій до складу однієї системи.

1.3. Аналіз принципів ідентифікації та аутентифікація користувача

Ідентифікація та аутентифікація користувача може бути проведена трьома способами, які відрізняються в відповідності із існуючими принципами і перевіряються ознаками (вони можуть використовуватися як окремо, так і спільно) [3, 4]:

– по власності (принцип «що ви маєте» – «*you have*»): перевіряється наявність у користувача певних речей або пристроїв (пропуск, пластикова карта, ключ, загальногромадянські документи, мобільний телефон та ін.);

– за знаннями (принцип «що ви знаєте» – «*you know*»): перевіряється наявність у користувача певних знань, до яких відносяться паролі, коди або конфіденційна інформація (наприклад, дівоче прізвище матері);

– за біометричними ознаками (принцип «хто ви є» – «*you are*»): перевіряються персональні фізичні властивості самого користувача (відбиток пальця, особа і т.д.).

Перші два методи, традиційні, не є вже надійними в тій мірі, яка потрібна на сьогоднішній день, адже ключі і карти доступу можуть бути вкрадені, загублені, або свідомо передані сторонній особі, пароль можна підглянути, перехопити і просто підібрати. Є тут і характерна особливість: паролі часто не зручні користувачам, особливо якщо політика безпеки вимагає застосування складних паролів (їх важко запам'ятовувати і вводити), в результаті чого нерідко на самому видному місці з'являються записи паролів (наприклад, прикріплюються до монітора). Часто, не усвідомлюючи їх важливості, співробітники передають особисті паролі колегам. Також багаторазово показана висока вразливість подібних систем аутентифікації для атак з використанням соціальної інженерії.

Природним кроком в підвищенні надійності стало використання коштів аутентифікації по біометричних ознаками [5], тому що в порівнянні з традиційними методами ідентифікації особистості біометричні мають ряд переваг.

Основні переваги біометричної ідентифікації:

– підвищена надійність обмеження доступу на об'єкти, що охороняються (через унікальність біометричних ознак достовірність ідентифікації дуже висока);

– виняток проникнень зловмисників за рахунок підробки або крадіжки документів, карт, паролів (біометричні ознаки набагато важче сфальсифікувати і практично виключається свідома або ненавмисна передача стороннім особам);

– мінімальні витрати і незручності, пов'язані з експлуатацією систем контролю доступу (виготовлення нових карт, ключів при їх втраті, псуванні; адміністрування на випадок забування паролів);

– забезпечення персональної відповідальності за використання ресурсів системи, що полегшує розслідування інцидентів;

– можливість організувати не тільки разовий облік доступу і відвідуваності співробітників, але і безперервний моніторинг.

Цілий ряд переваг, властивих біометричного підходу, зумовив його безумовне визнання, а здешевлення і вдосконалення обладнання – практично повсюдне впровадження біометрії протягом останніх двадцяти років. Так, якщо спочатку біометричні системи використовувалися тільки для обмеження доступу на особливо охоронюваних об’єктах (в основному військових), то зараз навіть на ноутбуках є сканери відбитків пальців користувачів, як пристрої контролю доступу до комп’ютера.

Високотехнологічні розробки, підкріплені біометричними дослідженнями, дозволяють втілити все більш зручні способи ідентифікації, зокрема, з використанням безконтактної технології. Зростає роль методів, які використовують поширене обладнання. Підвищується надійність ідентифікації і стійкість систем до атак.

Все більш прогресивні способи біометричної ідентифікації дозволили також значно розширити сферу застосування, дозволяючи ефективно вирішувати цілий ряд проблем практично у всіх галузях. Біометрія не тільки стала загальнодоступною, а й знайшла застосування при вирішенні цілого ряду нових завдань: управління персоналом (моніторинг робочого часу для обліку відвідуваності і погодинного нарахування зарплати), виявлення розшукуваних осіб в масово відвідуваних місцях, впізнавання постійних клієнтів в «системах доброзичливих продажів», голосове управління і ін.

Поряд з достоїнствами впровадження біометричних технологій, необхідно відзначити і певні складності.

1.4. Огляд літератури з проблеми ідентифікації людини по зображенню його особи

Дана стаття авторів Е. В. Єрьоміна, Ю. Х. Раджабова і А. А. Тельних представляє короткий огляд підходу до проблеми пошуку особи на фотографії і ідентифікації знайденого людини за допомогою методу головних компонент і алгоритму *Eigenface*. [3]

Стаття описує переваги методу головних компонент в контексті поставлених завдань, а саме: висока швидкість обробки та застосовність підходу до ідентифікації особи при різних кутах повороту і емоційного вираження.

Автори статті в доступній для розуміння формі описують етапи алгоритму і архітектуру свого рішення.

Важливою особливістю статті є математичний опис методу зменшення розмірності ковариационной матриці вибірки для знаходження її власних векторів і власних значень.

Предметом роботи дослідників *M. Turk* і *A. Pentland* Массачусетського Технологічного Інституту також є застосування методу головних компонент до проблем ідентифікації людини по зображенню його особи.

У цій статті йдеться більш детальне і глибоке опис математичного апарату розглянутого підходу і короткий опис застосування альтернативних методів, таких як нейронні мережі. Крім цього, автори демонструють свої експериментальні результати в точності ідентифікації при різних параметрах. [6]

3. Стаття «*Eigenfaces vs. Fisherfaces*: *Recognition Using Class Specific Linear Projection*». Відмінною особливістю даної роботи є опис альтернативного алгоритму *Fisherface* для ідентифікації. Автори *Peter N. Belhumeur, Joao P. Hespanha, and David J. Kriegman* описують підходи *Eigenface*, *Linear Subspaces* і *Fisherface* для розв'язання задачі ідентифікації і виділяють основні особливості кожного з підходів. [1]

Основним джерелом інформації з проблеми ідентифікації людини по аудіо-запису його голосу є книга *Beigi Homayoon* "*Fundamentals of speaker recognition*".

Перш за все, вона містить детальний розбір підходів до вирішення поставленого завдання. Крім цього автор зачіпає і інші близькі завдання, такі як верифікація, сегментація, класифікація і трекінг диктора. Книга містить детальну теоритических базу пропонованих методологій і порівняльний аналіз використання звуку та інших біометричний факторів в контексті завдання ідентифікації. Важливим аспектом є опис структури мовної системи і системи сприйняття звуку людини. [4]

Іншим джерелом, що дозволяє отримати базове розуміння принципу Мел-частотних кепстральних коефіцієнтів, є стаття *Vibha Tiwari "MFCC and its applications in speaker recognition*".

У цій статті йдеться огляд алгоритму отримання кепстральних коефіцієнтів з аудіо-сигналу. Будучи написаної доступною мовою, стаття стає придатною відправною точкою дослідження. [9]

1.5. Висновки до розділу

Сучасні біометричні системи вимірюють тільки одну з характеристик людини, що в ряді випадків викликає некоректну ідентифікацію. Побудова багатофакторних біометричних систем є очевидною перспективою, особливо при комбінації фізіологічних і поведінкових факторів.

Багатьма дослідниками виявлені критичні уразливості, що дозволяють навіть не дуже технічно оснащеним зловмисникам обходити системи біометричного захисту, як за рахунок перехоплення даних про легальних користувачів, так і за рахунок використання властивостей біометричних сканерів і особливостей програм. Ці уразливості, втім, усуваються з удосконаленням і появою нових типів сканерів і методів ідентифікації.

Також висловлюється побоювання, що для обходу біометричного захисту зловмисники будуть вимушено використовувати тяжкі кримінальні методи: крадіжки або підслуховування пароля вже не дозволяють заволодіти ідентифікатором, зате можливим способом стає ампутація частин тіла, або використання трупа.

На рівні кінцевого користувача існує стійке, підсвідоме упередження проти біометрії, викликане побоюванням порушення конфіденційності (наприклад, відтворення і застосування відбитків пальців на місці злочину). При цьому розробники апаратури змушені доводити, що зберігається не повна інформація, а лише побудований за характерними особливостями код, за яким можна відтворити фізіологічні дані.

Соціальний аспект впровадження біометричних технологій також останнім часом набуває все більшої значущості. Повсюдне поширення біометричних пристроїв і впровадження біометричних документів часто розглядається як крок до суспільства тотального контролю, порушення громадянських свобод. Найбільші нарікання викликають системи віддаленої і примусової прихованої ідентифікації, на зразок систем розпізнавання осіб в громадських місцях. Крім того, будь-який біометричний код несе в собі більше інформації, ніж потрібно, припустимо, для контролю доступу, тому висувається побоювання, чи не будуть вони використані проти громадян, порушуючи право на конфіденційність.

Але повсюдне проникнення біометричних систем в життя суспільства є вже незаперечним фактом. Всі світові аналітики прогнозують тільки підвищення попиту на біометрії в усіх галузях і розширення сфери її застосування.

РОЗДІЛ 2
ВИКОРИСТАННЯ АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ ЗА БІОМЕТРИЧНИМИ ПАРАМЕТРАМИ

2.1. Спеціальні технічні засоби обробки відеоінформації

З появою нових технічних рішень інтерес до відеоспостереження в торгівлі не згасає. Програмне поєднання чекової інформації з відеозображенням, що набуло широкого поширення в популярних системах відеоспостереження стало досить таки актуальним в сьогоднішньому світі. За своєю суттю воно призначене для застосування в магазинах самообслуговування, оснащених системами відеоспостереження і запису для контролю роботи касирів і запобігання шахрайству при оплаті товару.

Зазвичай в цих системах використовуються кольорові телекамери виробництва *KT&C KPC_S*520*DC* і *KPC S*523*DC*, оснащені якісними ПЗС матрицями виробництва *Sony*. Вони підбираються на початковому етапі, щоб відповідати вимогам замовника. Горизонтальний дозвіл складає близько 380 ТБ ліній при кольоровому зображенні, що цілком достатньо для контролю касових операцій. Як відомо, для відеоконтроля касових операцій необхідно щоб у полі зору телекамери знаходилося все, що потрібно побачити операторові, але при цьому телекамера не повинна фіксувати нічого зайвого. З того що повинне потрапляти у поле зору телекамери, потрібно відзначити наступне:

1) касовий апарат (контроль за розрахунковими операціями)

2) касир (для спостереження за його діями)

3) товар (для порівняння товару з інформацією чека)

4) візок або корзина покупця (для запобігання випадкам винесення товару з магазина без пред’явлення касирові)

Як видно на фотографії, узятій з відеоархіву системи, всі товари, що знаходяться на транспортній стрічці, виразно помітні, і їх легко дізнатися навіть в тих випадках, коли товари частково загороджені (в цьому випадку їх можна

розглянути по подальших або попереднім кадрам). Крім того, оператор, використовуючи інформацію чека, відразу бачить, який товар слід чекати на транспортній стрічці (рис. 2.1).

Рис. 2.1. Екран монітора системи відеоконтроля

Відеосигнал, отриманий від телекамер, встановлених над касами, поступає на пристрій, який здійснює апаратне поєднання інформації чека і відеозображення. Пристрій є пластиковою коробкою, на бічній стінці якої знаходиться роз'єм *DB*_15. До роз'єму приєднується кабель для підключення зовнішніх пристроїв. Кабель має два роз'єми *BNC* (або *RP*_406 *RCA*) для підключення вхідного і вихідного відеосигналу, а також роз'їм *DB*_9 для підключення до послідовного порту касового апарату і кубло для підключення адаптера живлення. На вхід пристрою подаються два незалежні сигнали: від касового апарату (про пробиваний чек) і телекамери. Потім програмно додається інформація чека в початковий аналоговий відеосигнал в реальному масштабі часу на рівні телевізійних рядків. На виході виходить звичайний відеосигнал що вже містить всю інформацію про касовий чек. Відеосигнал проходить через пристрій розпізнавання і при цьому не втрачає дозволу, хоча незначна частина відеоінформації все ж таки замінюється символами чека, але це не принципово. У іншому ж програмний пристрій, згідно проведеним вимірюванням, ніяк не змінює характеристики відеосигналу.

При подачі живлення і наявності вхідного відеосигналу програма здійснює накладення вікна з текстом чека від касового апарату на відеосигнал. Вікно чека є світлий напівпрозорий прямокутник, в якому виводяться символи чорного кольору. Є можливість висновку і з світлими символами, але найчастіше, як і в нашому випадку, використовується чорний колір. Навіть на повністю чорному фоні всі символи будуть виразно помітні, оскільки вікно чека напівпрозоре. Розмір вікна при необхідності можна збільшити на екран або набудувати положення вікна чека в будь-якому зручному місці екрану. При виведенні символів чека на принтер касового апарату вони приймаються програмою, обробляються і виводяться у вигляді тексту у вікно відповідно до опису символів в знакогенераторі. Якщо вибрана ширина вікна менше, ніж довжина рядка чека (наприклад з міркувань наочності), то останні в рядку символи не виводяться на екран. Перенесення в даному випадку не вимагається, оскільки стрічка касового апарату вузька.

Після заповнення всіх рядків вікна відбувається вертикальний зсув інформації у вікні: самий нижній рядок переміщається на одну вище, а верхня зникає, тобто створюється повна аналогія віртуальним чеком. Інформація при цьому не може загубитися навіть у разі дуже низької швидкості запису (0.5 к/с). Хоча нижні рядки поступово змінюють верхні, касир не в змозі так швидко пробивати товар, оскільки потрібно не просто передати товар, але ще і сканувати його штрих код. Коли висновок на принтер припиняється, то після закінчення часу утримання вікна, вікно з інформацією про чеку зникає з екрану. При відновленні друку вікно з’являється в тому вигляді, в якому воно було до зникнення. Висота вікна чека підбирається експериментально з урахуванням швидкості запису (низька швидкість запису кадрів – високе вікно). Всі вищеперелічені параметри зберігаються в незалежній пам’яті пристрою і не вимагають перезавантаження при пропажі живлення. Параметри задаються при підключенні програмного пристрою до комп’ютера, для цього разом з пристроєм поставляється програмне забезпечення.

Окремо потрібно сказати про те, яким чином інформація касового чека потрапляє у вікно програми. Очевидно, що ця інформація береться з

послідовного порту касового апарату. Але тонкість полягає в тому, що краще не використовувати той порт, до якого підключений касовий принтер. Хоча це дуже поширене рішення (в цьому випадку ставиться розгалуджувач на послідовний порт, до якого підключений касовий принтер), але його не можна назвати оптимальним. Оскільки більшість касових апаратів мають декілька послідовних портів, то хоч би один з них виявиться вільним (зазвичай в касовому апараті присутні 2–4 послідовних порту). Наприклад, в цьому супермаркеті *Oskar* були встановлені багатопортові касові апарати *NCR* 7454 що мають по 4 послідовних порту. Використовуючи вільний порт, можна обійтися без розгалуджувачів і тим самим понизити вартість встановлюваного устаткування (при великій кількості касових апаратів економія може бути дуже істотною). Звичайно, в деяких касових апаратах з 2 послідовними портами обидва порти можуть виявитися зайнятими, і в цьому випадку вже не вдасться обійтися без розгалуджувачів, але їх потрібно ставити не на той порт, до якого підключений принтер касового апарату, а на іншій. Причина криється в тому, що з погляду податкової інспекції неправомірно втручатися в передачу даних від касового апарату до принтера. Очевидно, що розгалуджувач ніяк не порушує передачу даних, але, проте, у податкових інспекторів вже сформувалося украй негативне відношення до розгалуджувачів, встановлених на порту принтера касових апаратів.

В даний час не існує якої-небудь прямої директиви, що забороняє використовувати такий спосіб отримання чекової інформації, але не можна виключити можливості її появи.

Для того, щоб здійснити виведення чекової інформації на додатковий

послідовний порт паралельно з виведенням інформації на послідовний порт, до якого підключений принтер, проводиться незначне оновлення програмного забезпечення касового апарату. У випадку з касовими апаратами *NCR* 7454, які були встановлені в супермаркеті, йдеться об все лише про додавання однієї строчки в основний програмний код касового апарату. У ре зультате вийшло дуже просте і витончене рішення, що не вимагає ніяких розгалуджувачів.

На рисунку 2.2 зображено принцип роботи системи стеження за касовими операціями.

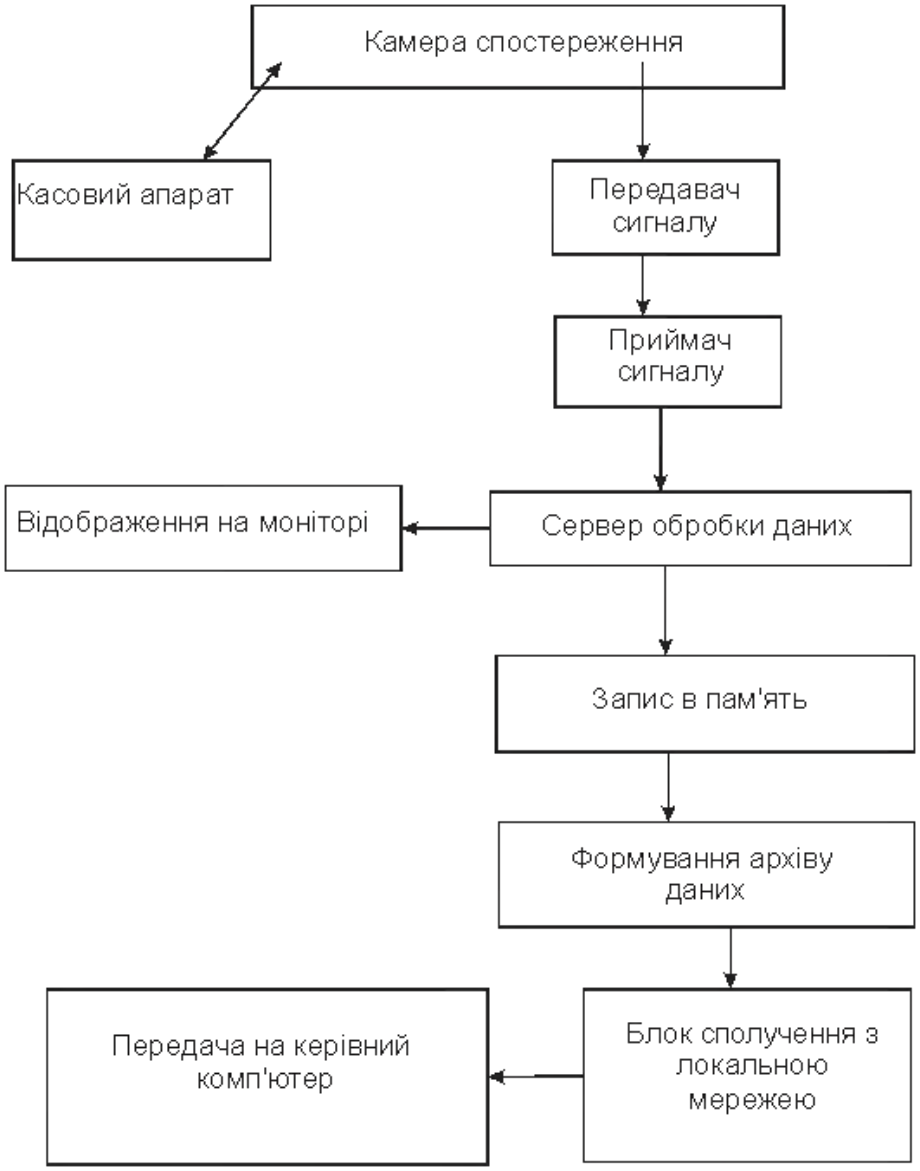

Рис.2.2. Принцип роботи системи стеження за касовими операціями

Оскільки програма працює з широко поширеним *Epson* сумісним протоколом касових принтерів, який використовується в значній частині касових апаратів, присутніх на вітчизняному ринку, то список сумісного устаткування повинен бути вельми широкий і проблем з інтеграцією з існуючими касовими апаратами не повинно виникати. В цілому, можна інтегрувати практично будь-які касові апарати за виключенням хіба що автономних касових апаратів, які не здійснюють взаємодії з системами автоматизації торгівлі і не передають ніякої інформації: якщо з касового апарату не видається ніякої інформації, то її не

можна і отримати. Як показує приклад проведеної інсталяції, програма легко вбудовується в існуючу інфраструктуру магазина і не впливає на працездатність системи відеоспостереження і расчетно–кассовой системи. Єдиною умовою застосування є наявність в касовому апараті послідовного порту, на який може бути виведена інформація про друкований чек. Відеосигнал, суміщений з інформацією чека, поступає в комп'ютерну систему відеоспостереження і запису. Телекамери, встановлені над касами і в торговому залі обробляються єдиною комп'ютерною системою, і з міркувань зручності роботи оператора недоцільно створювати окрему систему відеоспостереження і запису для контролю касових операцій і окрему систему для обробки решти телекамер. На монітор оператора виводиться нестисле зображення з високою якістю, а на жорсткі диски записується вже стисле зображення. Як відомо, комп'ютерна система може записувати повний кадр *PAL* з максимальним дозволом 768x576 пікселів, але з міркувань економії дискового простору і на вимогу замовника може бути зменшений.

Для запису і відображення телекамер на один супермаркет зазвичай встановлюється 2 сервери (16–24 канали на сервер). Для ефективнішого використання дискового простору сервери об'єднані по локальній мережі, при заповненні жорстких дисків на одному сервері відеоархів продовжує записуватися на жорсткі диски іншого сервера.

2.2. Програмні системи розпізнавання обличчя

Так, в США систему розпізнавання осіб стали активно упроваджувати і тестувати в аеропортах після сумно відомих подій 11 вересня. У тих же Сполучених Штатах ця технологія застосовується на стадіонах при проведенні крупних спортивних заходів, таких, наприклад, як Кубок США по американському футболу. У Великобританії в передмісті Лондона працює система розпізнавання осіб з підключеними до неї 250 телекамерами. Система автоматично вихоплює зображення осіб людей, що йдуть по вулиці, і порівнює ці зображення з комплектом фотографій злочинців, що знаходяться в розшуку. З

аналогічною метою використовує систему розпізнавання осіб і поліція США, наприклад, в містечку Вірджинія Біч, штат Вірджинія. Перші результати тестування системи розпізнавання при ідентифікації тимчасово затриманих осіб в шотландському місті Грампіане продемонстрували цінність цієї технології.

Система розпізнавання осіб – це система біометричної ідентифікації людини по зображенню його обличчя, що складається з і двох модулів – захоплення і розпізнавання. В цілому система діє таким чином.

Телекамера отримує зображення. Кожен кадр поступає в модуль захоплення, де відбувається перевірка зображення на наявність в нім одного або декількох осіб. Якщо особи виявлені, то для кожної особи визначається його розмір і розташування. Захоплення відбулося (рис.2.3).

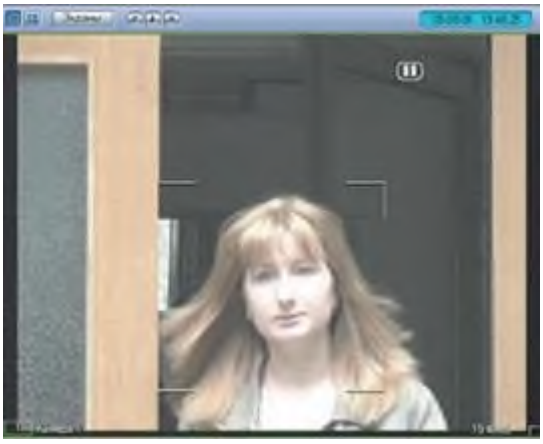

Рис. 2.3. Захоплення обличчя в програмному додатку

Після цього в дію вступає модуль розпізнавання. Спочатку він визначає положення центрів очей людини на зображенні. Далі з обличчям відбувається приблизно те ж, що і з головою героя якого-небудь мультфільму – особа повертається строго у фас, і розмір його зменшується або збільшується так, щоб центри очей розташувалися в двох певних крапках. Відбувається «нормалізація» зображення особи. Наступний крок – робота над яскравістю, контрастністю і іншими параметрами зображення, цілком аналогічна тому, що можна зробити з картинкою за допомогою сучасної дизайнерської програми.

Після цього модуль розпізнавання переходить до вимірювання певних параметрів особи – тих, по яких можна відрізняти одну людину від іншого. Параметри ці підібрали і заклали в алгоритм розпізнавання розробники модуля.

Зрозуміло, зворотна процедура – отримати зображення особи на основі його параметрів – вже не може бути виконана. Набір параметрів, витягнутих із зображення особи, – це біометричний образ обличчя людини. Щоб система «*Face*-інтелект» могла встановити, чиє зображення потрапило в кадр, вона порівнює біометричний образ даної особи з набором таких же образів, про які наперед відомо, кому вони «належать». З таких образів складаються всілякі бази даних – співробітників підприємства, осіб, оголошених в розшук, важливих персон і т.д. Результат порівняння виражається в коефіцієнті розпізнавання, що визначає ступінь схожості захопленої особи і образу в базі (рис. 1.3). У результаті програма ухвалює рішення про те, що це – одна і та ж особа, якщо коефіцієнт достатньо великий. При цьому можна регулювати той поріг, якого повинен досягати коефіцієнт розпізнавання, щоб було ухвалено таке рішення. Реакція на результат розпізнавання залежить від застосування системи. Якщо йдеться про спробу відсіяти терористів в аеропорту при огляді, то система повинна повідомляти оператора про те, що коефіцієнт розпізнавання великий, тобто просто привернути його увагу. На прохідній підприємства, де одні і ті ж люди проходять багато раз, спільна робота системи розпізнавання осіб і системи контролю доступу може бути повністю автоматизована: якщо особа схоже на одне з тих, хто є в списку співробітників, то прохід вирішується.

Є в системі і деталізований монітор розпізнаних осіб. На нім зліва відображається особа, захоплена телекамерою, а також інформація про дану персону. Справа, в ряд – список схожих кандидатів по убуванню ступеня схожості, з вказівкою ступеню схожості і особистої інформації про кожне (рис.2.4).

Існує можливість пошуку розпізнаної персони у відеоархіві і проглядання відеоролика, в якому присутня розпізнана особа. У інтерфейсі, призначеному для пошуку людей по зображенню, указується період часу для пошуку і фільтри для параметрів пошуку. Після виконання запиту на екран виводяться ті, що задовольняють умовам пошуку запису в протоколі.

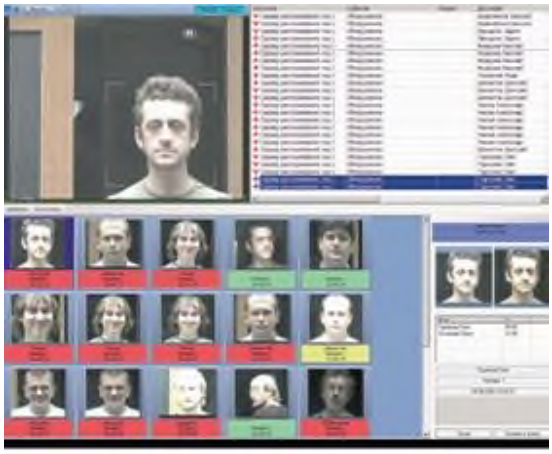

Рис. 2.4. Вікно додатку ідентифікації осіб

Необхідно акцентувати увагу ще на одній відмітній властивості комплексу «Інтелект» – розподіленості системи. Ця перевага властива і всім продуктам, розробленим на його базі. У програмі розподіленість реалізована таким чином: телекамери, які отримують початкове зображення, можуть бути встановлені в різних місцях, віддалених один від одного, при цьому захоплення осіб і їх розпізнавання можуть виконуватися на різних серверах, а бази даних, які використовуються для розпізнавання, можуть також знаходитися на одному або на декількох серверах. Крім того, оскільки розпізнавання – це ресурсоємна операція, для сервера розпізнавання можна виділити окремий комп'ютер, на якому не буде нічого, окрім самого сервера розпізнавання.

На рисунку 2.5 зображена блок схема роботи системи стеження і розпізнавання осіб.

В цілому застосування системи розпізнавання осіб визначається її особливостями, відмінностями від інших біометричних технологій, тобто технологій, які для ідентифікації людини використовують його ознаки, особливі для кожного індивідуума. По надійності розпізнавання осіб поступається деяким іншим біометричним технологіям, зокрема двом найбільш відпрацьованим і доведеним до практичного рівня – ідентифікації людини по відбитках пальців і по веселковій оболонці ока. При цьому головна перевага розпізнавання осіб полягає в тому, що воно не вимагає яких-небудь дій з боку людини, що перевіряється.

Рис. 2.5. Функціональна схема роботи системи в 24-х камерному

Характерним прикладом використання системи розпізнавання осіб є її інтеграція з системою контролю доступу на підприємствах, в організаціях і установах. Особливою перевагою такого тандему є посилювання заходів безпеки і контролю. Недоліком системи контролю доступу є можливість маніпуляції з картками доступу – їх можна передавати іншим людям, красти, втрачати. Саме цей недолік безболісно компенсує система розпізнавання осіб.

Програма прочитує з картки прізвище її законного власника і знаходить в базі даних його фотографію. Потім він розпізнає обличчя людини, що стоїть перед телекамерою, і порівнює його з фотографією, витягнутою з бази. Такий подвійний контроль гарантує неможливість маніпуляції з карткою доступу.

Інший характерний приклад – це використання ідентифікації людини по зображенню його обличчя в аеропорту. Тут паралельно з оглядом речей перевіряють обличчя пасажира, порівнюючи його зображення з наявними в базі даних знімками. Як наголошувалося вище, подібна система вже функціонує в деяких зарубіжних аеропортах. Причому аеропорти обмінюються власними сформованими базами даних, що багато разів збільшує можливість знайти шукану людину. Наприклад, громадянина, що зробив правопорушення під одним прізвищем, можна знайти, коли він проходитиме контроль наступного разу вже під інший.

Ще однією групою об’єктів, де дуже актуальне використання системи розпізнавання осіб, є торгові підприємства і розважальні заклади. Магазини, супермаркети, автозаправки, клуби, ресторани, кафе – всіх їх об’єднує одне: бажання витягнути максимальний прибуток, для чого необхідно підвищувати якість обслуговування клієнтів і забезпечити відвідувачів. Для них важливо обмежити доступ людям, які з тих або інших причин небажані в цьому закладі і, навпаки, наперед дізнавшись про прибуття постійного клієнта або *VIP*-персони, як можна на більш високому рівні обслужити його.

Аналогічні системи багатофакторної ідентифікації на сьогоднішній день найчастіше мають поширення в сфері виробництва, входячи в комплекс продуктів для аутентифікації, наприклад, в охоронних системах. Такі системи зазвичай вимагають додаткового більш точного обладнання для зняття зразків, прикладами можуть служити *IFace*202 і *Multi-Bio* 700, вироблені *ZKSoftware*.

Обидві згадані системи являють собою термінали багатофакторної ідентифікації, працюють з фотографіями осіб, відбитками пальців і іншими атрибутами.

Плюсом таких систем є висока надійність, обумовлена спеціально розробленим обладнанням. До мінусів можна віднести необхідність і габарити додаткового пристрою, обмеженість розширення функціоналу, вартість.

Також існує набір програмних продуктів, які не вимагають складного устаткування, а використовують стандартні веб-камери і мікрофони. Однак зазвичай такі програми ґрунтуються на одному з чинників. Так, наприклад, програма *FastAccess* від компанії *Logitech* пропонує ідентифікацію та управління паролями на основі зображення особи. *GritTec Laboratory* надає програмний комплекс для ідентифікації по голосу (табл. 2.1).

Таблиця 2.1

Порівняння аналогів систем ідентифікації за біометричними параметрами

Назва системи	Багатофакторність	Необхідність додаткового обладнання	Оцінка простоти використання (0-5)
*IFace*202	Зображення, відбитки пальців, карта	Необхідний додатковий термінал	4
Multi-Bio 700	Зображення, відбиток пальців, карта, пароль	Необхідний додатковий термінал	3
FastAccess	зображення	Стандартна веб-камера	5
GraitTec lab.	звук	Стандартний мікрофон	2

2.3. Особа як біометричний ідентифікатор

Практика показує, що для пересічних користувачів, які застосовують у себе системи біометричної ідентифікації і аутентифікації, дуже важливо зручність застосування цих засобів (це не тільки швидкість і простота проведення процедури, але і можливість використання звичного обладнання). Більшість експертів сходяться в тому, що в зв’язку з цим актуальні лише три методу

розпізнавання: за відбитками пальців, райдужною оболонкою або особі, вибір між ними робиться в залежності від постановки задачі.

На сьогодні оптимальним співвідношенням між надійністю аутентифікації, ціною і зручністю використання має визначення особистості по обличчю, чим і пояснюється високий темп розвитку і поширення таких технологій.

2.3.1. Реалізація систем розпізнавання обличч

Розпізнавання обличчя – найбільш древній і поширений спосіб ідентифікації, заснований на тому, що риси обличчя і форма черепа кожної людини індивідуальні, люди пізнають один одного в першу чергу по обличчю. По суті, саме така процедура виконується, коли ми, наприклад, пред'являємо свій паспорт на пропускному пункті. Перевіряючий (вахтер, прикордонник, провідник поїзда) звіряє фото в паспорті з особою власника паспорта і приймає рішення – його це паспорт чи ні. 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,

Необхідно відзначити, що останнім часом розроблені деякі інші методи розпізнавання, що виконують сканування особи, наприклад, розпізнавання осіб в інфрачервоному світлі по термограмме особи. У зв'язку з цим назву розглянутого методу часто уточнюють: як правило, його називають ідентифікацією по геометрії особи (або «розпізнавання обличчя»). Втім, якщо додаткового уточнення не проведено, мається на увазі саме цей метод, як історично перший і найбільш поширений.

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

– не потрібно безпосереднього контакту людини, особа якого встановлюють, зі сканером (людині не потрібно залишати відбитки пальців, дивитися в об'єктив або вимовляти якісь слова), за винятком систем

розпізнавання осіб 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, де не потрібна спеціальна техніка (застосовуються стандартні камери відеоспостереження);

– це єдиний біометричний спосіб ідентифікації з точки зору можливості багатоцільового застосування;

– при ідентифікації використовується загальнодоступна біометрична характеристика, зазвичай не приховувана людиною (це важливо з урахуванням конфіденційності інших біометричних даних, наприклад, відбитків пальців).

Принцип роботи біометричних систем розпізнавання по обличчю повністю відповідає наведеним раніше алгоритму (див. Розділ 1.1). За допомогою фото- або відеокамери робиться знімок людини, зображення спеціальним чином обробляється, що ви можете виділити на кадрах обличчя людини і оцифровувати його. На отриманому зображенні особи виділяється велика кількість індивідуальних параметрів (так звані базові точки: вилиці, форма очей, перенісся, контур губ і т.д.). В результаті кожна особа описується унікальним набором параметрів, причому навіть з деяким надлишком. Зазвичай задається близько 2000 оціночних параметрів, тоді як для ідентифікації з високим ступенем точності потрібно всього кілька десятків базових точок (не більше 40 характеристик). За отриманими даними (по знімку або декільком знімкам), відповідно до використовуваним способом кодування, в цифровій формі будується образ особи, для порівняння з еталоном. Фотографія і цифрове опис особи заносяться в базу даних, з якої згодом порівнюється распознаваемое особа.

Хоча особа людини і унікальний параметр, але досить 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 (різні кути повороту голови, зміни нижньої частини обличчя при

вимові ключового слова і т.д.) зчитувальних образів може варіюватися в залежності від алгоритмів і функцій системи, що реалізує даний метод (рис. 2.6).

Рис. 2.6. Приблизний еталонний набір оцифрованих образів особи

Всі безліч методів розпізнавання по геометрії особи ділиться на два напрямки: 2*D* і 3*D* методи розпізнавання [8]. У кожного з них є переваги і недоліки, проте багато що залежить ще і від області застосування і вимог, пред'явлених до конкретного алгоритму.

Метод Розпізнавання особи в 2*D* з'явився досить давно і бере початок в криміналістиці (словесний портрет, фоторобот), що сприяло його початкового розвитку.

Розпізнавання обличчя спочатку мало неприйнятно низьку в порівнянні з іншими методами надійність, яку можна порівняти з надійністю розпізнавання голосу. Високі результати досягалися лише при фіксованих зовнішніх факторах (ракурс, освітленість, дальність і т.п.). Згодом він став більш надійним, але кардинально статистичні характеристики алгоритму не покращали: це як і раніше один з найбільш статистично неефективних методів біометрії, безумовно поступається іншим. Головний недолік 2*D* розпізнавання особи – недостатньо висока статистична достовірність – нівелює переваги методу. В даний час з-за слабких статистичних показників він впевнено застосовується лише в багатофакторної (або перехресної) аутентифікації, або в соціальних мережах (наприклад, вказівка людей на фото в «*Facebook*»).

Крім того, згідно з наявною статистикою, в задачах ідентифікації при використанні великих баз даних надійність і швидкодію таких біометричних систем різко знижується [6], змушуючи використовувати додаткові ознаки для аутентифікації.

На практиці також пред'являються вимоги до висвітлення (наприклад, не вдається реєструвати особи входять з вулиці людей в сонячний день), відсутності зовнішніх перешкод (як, наприклад, окуляри, борода, деякі елементи зачіски). Обов'язково фронтальне зображення особи з вельми невеликими відхиленнями, багато алгоритми 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 320×240 пікселів на дюйм, які передають дані зі швидкістю відеопотоку, принаймні 3-5 кадрів в секунду. Нові можливості цифрового відео і мультимедійних цифрових технологій вивели якість ідентифікації на якісно новий рівень. Інтенсивний розвиток і, як наслідок, їх здешевлення дозволяють впровадити їх в широке повсюдне використання.

Система працює з відносно простим двовимірним зображенням, що помітно спрощує алгоритми і знижує інтенсивність обчислень. Втім, навіть в цьому випадку завдання розпізнавання все ж не тривіальна.

В даний час існує чотири основні методи розпізнавання особи, які розрізняються складністю реалізації та метою застосування [5]:

– метод автоматичної обробки зображення особи;

– «*Eigenfaces*» (нім. «Власне обличчя»);

– аналіз відмінних рис;

– аналіз на основі нейронних мереж.

Метод автоматичної обробки зображення особи – найбільш проста технологія, що аналізує відстані і ставлення відстаней між легко визначаються точками особи. Особливо важливі характерні частини обличчя, а також ті, які практично не змінюються з плином часу: верхні обриси очниць, очі, області навколишні вилиці, кінець носа, куточки рота (рис. 2.7).

Хоча даний метод не дуже потужний, він може бути досить ефективно використаний в умовах слабкої освітленості.

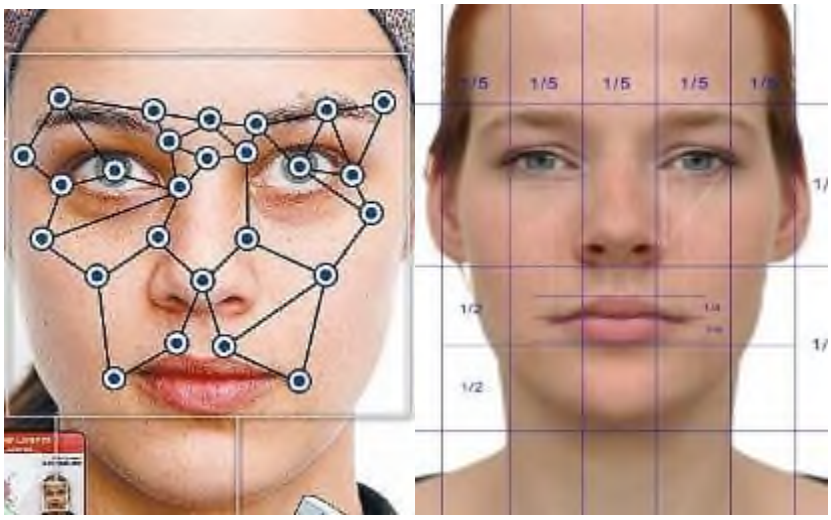

Рис. 2.7. Ілюстрації методу ідентифікації, заснованого на аналізі характерних точок і відстаней

Технологія «*Eigenface*» використовує представлення зображення особи в градаціях сірого у вигляді статистично обґрунтованих, стандартних блоків даних (областей особи). Даний метод заснований на тому, що всі особи можуть бути отримані з репрезентативної вибірки осіб з використанням сучасних статистичних прийомів (аналогічно тому, як це робиться при створенні фоторобота). Вони охоплюють пікселі зображення особи і універсально представляють особові форми (двомірні зображення-шаблони). Фактично в наявності є набагато більше елементів побудови особи, ніж кількість самих частин обличчя. Однак виявляється, що синтез даної особи з високою точністю вимагає тільки 12-40 характерних елементів з повного доступного набору. Комбінуючи 100-120 різних шаблонів, можна уявити велику кількість осіб. При реєстрації вигляд кожної конкретної людини представляється у вигляді ряду 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. 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. 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 характерних рис подібна методиці «*Eigenface*», але в більшій мірі адаптована до зміни з часом зовнішності або міміки людини. У технології «відмінних рис» використовуються не тільки характерні особливості областей особи, а й враховано їх відносне положення. Особа людини унікально, але досить динамічно. Наприклад, при посмішці спостерігається деяке зміщення частин обличчя, розташованих біля рота, а також рух суміжних частин. Ідентичність особи визначається не тільки характерними елементами, але і способом їх геометричного об’єднання (тобто враховуються їх відносні позиції). Індивідуальна комбінація цих параметрів визначає особливості кожної конкретної особи.

Наприклад, подібний алгоритм, розроблений в Університеті Рокфеллера, лежить в основі програми *FaceIt* компанії *Visionic*.

У методі, заснованому на нейронної мережі, характерні особливості зареєстрованого і перевіряється осіб порівнюються на збіг. Нейронні мережі встановлюють відповідність унікальних властивостей людини, а потім за допомогою відповідних вагових коефіцієнтів кожної характеристики визначає

ступінь загального відповідності особи, що перевіряється еталону. Метод має високу якість ідентифікації в складних умовах.

Технологія нейронних мереж використовується в системі розпізнавання осіб *TrueFace* компанії *Miros*.

Для порівняння з графічними зображеннями-шаблонами застосовуються два основних алгоритму порівняння: мінімальної середньої кореляційної енергії (*MACE*) [11] і Локальні Бінарні Шаблони (*LBP*) [12].

Локальні Бінарні Шаблони (*LBP*) використовують обробку околиці пікселя цифрового зображення (рис. 2.8). Метод *LBP* популярний для розпізнавання графічного зображення в цілому, а останнім часом застосовується і для розпізнавання осіб. Непараметричне ядро *LBP* аналізує піксельну структуру зображень. Воно інваріантної до монотонним сіро-масштабних перетворень, тобто менш чутливо до освітленості, що вельми важливо.

Рис. 2.8. Ілюстрації принципу дії методу *LBP*, заснованого на аналізі піксельної структури зображень

Принцип роботи *MACE*-фільтра заснований на визначенні середнього ступеня кореляції до заздалегідь підготовленим 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 в базі потрібно порівняно велика кількість зображень особи, в різних умовах освітлення і зміни міміки. У разі використання MACE фільтра виникає помилка визначення особи> 2%.

Реалізація розпізнавання обличчя в 3*D* являє собою досить складну математично і технічно завдання. В даний час існує безліч методів по 3*D* розпізнаванню особи. 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 (рис. 2.9).

Рис. 2.9. Ілюстрація побудови тривимірного образу особи
і характерних точок на ньому

Класичним вже методом є метод проектування шаблону. Він полягає в тому, що на обличчя проектується світлова сітка. Луч, що падає на викривлену поверхню, згинається – чим більше кривизна поверхні, тим сильніше вигин променя. Спочатку при цьому застосовувався джерело видимого світла, що подається через «жалюзі». Потім видиме світло був замінений на інфрачервоний, що має ряд переваг. Далі камера робить знімки зі швидкістю десятки кадрів в секунду, а отримані зображення обробляються спеціальною програмою. За отриманими знімками відновлюється 3*D* модель особи, на якій виділяються і віддаляються непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі – виділяються антропометричні особливості, які записуються в унікальний код, заносячи в базу даних.

Крім низької чутливості до зовнішніх чинників, як на самій людині, так і в оточенні (освітленість, поворот голови), найважливішою перевагою методу є високий рівень надійності. Вважається, що статистична надійність методу порівняння з надійністю ідентифікації за відбитками пальців. Наприклад, для кращих моделей фірми *Bioscript* (3*D EnrolCam*, 3*D FastPass*), що працюють за методом проектування шаблону при *FAR* = 0.0047%, *FRR* становить 0.103%. Зміни міміки обличчя і перешкоди на обличчі погіршують статистичну надійність методу. Час захоплення і обробки зображення близько 1-2 секунди для кращих моделей. Недолік – дорожнеча обладнання. Наявні комплекси перевершували за ціною навіть сканери райдужної оболонки. Метод ще недостатньо добре розроблений, що ускладнює його широке застосування.

Також набирає популярність метод 3*D* розпізнавання по зображенню з декількох камер. Цей метод дає точність позиціонування вище, ніж у методу проектування шаблону. Прикладом може бути 3*D*-сканер фірми *Vocord*. Комерційні системи, втім, ще не анонсовані.

Перехідний метод реалізує накопичення інформації. Тут, так само як і при 2*D*, використовується одна камера. При занесенні суб'єкта в базу суб'єкт повертає голову, і алгоритм з'єднує зображення воєдино, створюючи 3*D* шаблон. А при розпізнаванні використовується кілька кадрів відеопотоку. Цей метод має кращі характеристики, ніж 2*D* метод, але є експериментальним.

2.3.2. Методи аудіо-ідентифікації

Вперше мел-шкала була представлена Ньюманом, Стивенсом і Волкманом в 1937, як нове логарифмічна уявлення звуку, більш точно відображає його сприйняття людським вухом.

Значення в 1000 *mel* ставиться у відповідність частоті 1 *Khz*. Переклад з частотного подання в крейда проводиться за такою формулою [5]:

$$m = 2595 \cdot log_{10}(1 + \frac{f}{700}),$$

де f – значення частоти звуку.

Мел-частотні кепстральних коефіцієнти – набір значень на крейда-шкалою, що містить тільки унікальну і значиму інформацію вихідного сигналу.

Для отримання крейда-частотних кепстральних коефіцієнтів по сигналу необхідно зробити наступні дії [2,4,9]:

1. Сигнал розбивається на перекриваються вікна довжиною 25 – 30 мс. Тривалість вікна вибирається таким чином, щоб мінімізувати коливання частоти всередині її кордонів, але залишити можливість подальшої обробки.

2. Виробляється перетворення Фур'є для отримання спектра сигналу.

3. Накладається набір фільтрів. На даному етапі спектр сигналу розподіляється між трикутними крейда-частотними вікнами.

Цей процес симулює неможливість людського вуха розрізняти близько розташовані частоти.

Для отримання такого розподілу кожен вектор спектра множиться на віконну функцію.

В результаті виходить набір значень енергії сигналу, які відповідають частотним вікнам.

1. Проводиться логарифмирование кожного значення енергії.

2. Проводиться дискретне косинусное перетворення для отримання шуканих коефіцієнтів.

Метод векторної квантування спочатку використовувався в задачах стиснення аудіо і відео даних.

В рамках завдання розпізнавання диктора ця техніка розподіляє *k*-мірні вектора особливостей векторного простору за кінцевим набору областей Вороного. Розподіл проводиться алгоритмом кластеризації, наприклад, *k-means*.R^k

У кожного класу є середній вектор – центр ваги або кодове слово. Набір всіх кодових слів формує кодовий довідник.

Приклад кластеризації наведено на рисунку 2.9 [4,8].

Кластеризація може здійснюватися за допомогою алгоритму *k-means* або алгоритмом Лінде-Бузо-Грея [4]. Після чого, на етапі ідентифікації, знаходиться найбільш близький кластер до тестового сигналу.

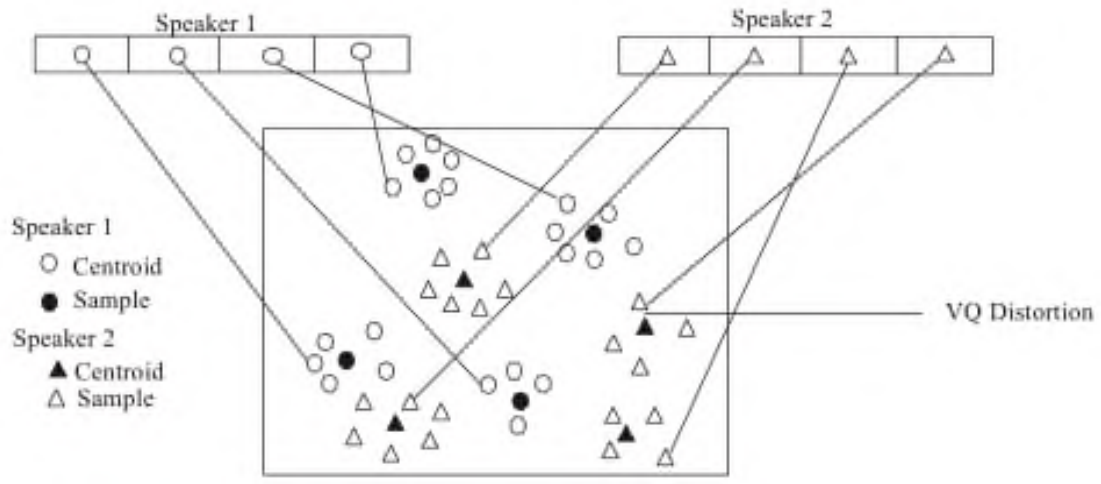

Рис. 2.9. Приклад кластеризації кодового словника

2.4. Висновки до розділу

Здебільшого компанії вважають за краще розвивати готові системи, включаючи сканери, сервери і ПЗ. Однак є й ті, хто пропонує споживачеві тільки *SDK*. Також з'явилася нова група компаній, рішення яких називаються *middleware*. Це «програмне забезпечення – посередник» між кінцевим обладнанням та програмними системами, в які інтегруються процедури біометричної ідентифікації. Причому *middleware* може реалізувати як просто вхід в систему з використанням вимірювань біометричного сканера (наприклад, *Windows Logon*), так і самостійний функціонал, наприклад створення криптографічних контейнерів за допомогою ключа, одержуваного тільки за певним відбитком пальця.

Загальновизнаним фактом є те, що в сучасному постіндустріальному світі основним активом стає інформація, причому прогресуючими темпами зростає її концентрованість, тобто одна людина задіяний в обробці все більшого обсягу інформації. При цьому неминуче зростає значення таких аспектів, як інформаційна безпека, контроль доступу і моніторинг діяльності, якість яких прямо визначається надійністю аутентифікації.

Важливою тенденцією є те, що для підвищення точності виробляють об’єднання кількох різних алгоритмів, які аналізують особа. Наприклад, доповнюють розпізнавання особи розпізнаванням особистості по вушній раковині, яка забезпечує високий відсоток збігу. У разі спільного алгоритмів ймовірність вірного розпізнавання стабілізується, взаімоісключая неточності роботи окремих алгоритмів. Варто відзначити, що не завжди доцільно використовувати велику кількість алгоритмів, так як приріст ймовірності розпізнавання може бути не суттєвий.

Очевидна тенденція і розширення застосовності розпізнавання осіб: з’являється все більше комбінованих систем. Наприклад, інтелектуальна система відеоспостереження з функцією ідентифікації людей веде спостереження 24 години на добу, в той час як людська увага починає слабшати після декількох хвилин спостереження за зображенням на моніторі. Аналізуючи потрапили в кадр події, вона може попередити про візит високопоставлених гостей або дати знати про появу шахраїв в казино або хуліганів на стадіонах.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ ЧЕРЕЗ РОЗПІЗНАВАННЯ ГРАФІЧНИХ ТА АУДІО ФАЙЛІВ

3.1. Інструменти реалізації

Дана програма багатофакторної біометричної ідентифікації людини була розроблена на мові *Java,* в середовищі розробки *Intellij Idea*. Для вирішення деяких завдань в процесі розробки були використані наступні сторонні бібліотеки:

– *Sarxos Webcam* – бібліотека, яка забезпечує доступ до підключеним веб-камерам і захоплення зображення з них;

– *Slf4j, log4j* – бібліотека розширених можливостей логування, використовується *Sarxos webcam*;

– *Bridj* – бібліотека взаємодії з драйверами веб-камери, використовується *Sarxos webcam*;

– *Apache common math* 3 – математична бібліотека;

– алгоритм *Fast Fourier Transform* [10].

3.2. Структура програми

Вся система ідентифікації розбита на три логічних модуля: модуль ідентифікації по зображенню, модуль ідентифікації по голосу, модуль зберігання даних і інтерпретації результатів.

Взаємодія користувача з програмою організовано через графічний інтерфейс.

Структура програми відображена на рис. 3.1.

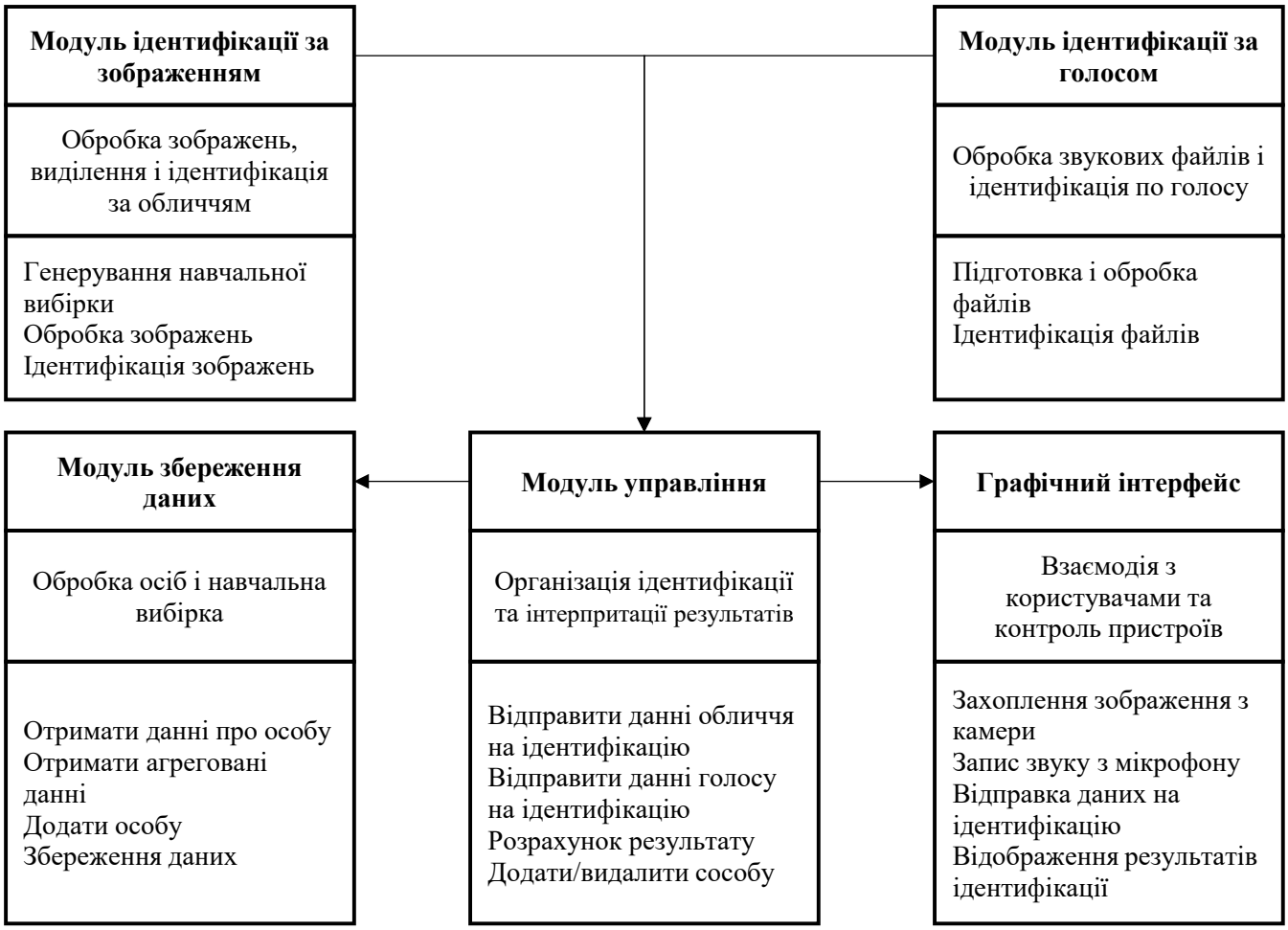

Рис. 3.1. Зв’язки модулів програми

3.2.1 Модуль ідентифікації по зображенню

Основою даного модуля є алгоритм *Eigenface*, який виробляє ідентифікацію на підготовлених даних у вигляді векторів зображень. Також даний модуль включає в себе алгоритми попередньої обробки растрових зображень в форматі *PGM* і *PNG*:

На вхід алгоритму навчання надходить матриця, складена з векторів всіх зображень всіх користувачів. Всі вектори мають однакову розмірність, при роботі з наявною вибіркою зображень з розмірами 92×112 точок, вектори мають довжину 10304 і зберігають цілочисельне значення інтенсивності сірого кольору від 0 до 255.

Навчання відбувається кожного разу після додавання нового людини або зображення в базу. По завершенні навчання матриця записується на жорсткий диск і вивантажується з оперативної пам’яті.

На вхід алгоритму ідентифікації подається цілочисельний вектор тестового зображення, що має формат ідентичний векторах навчальної вибірки. Проводиться визначення вектора, найближче розташованого до даного тестового вектору. При тестуванні різних підходів до розрахунку відстані були отримані результати, що свідчать про те, що квадрат Евклидова відстані показує кращу якість виділення ідентифікованого зображення серед всієї вибірки в порівнянні з відстанню Махаланобіса.

Емпірично на основі 40 експериментів було вибрано порогове значення відстані в 10^6.

На виході є індекс знайденого зображення в навчальній матриці і відстань до нього від тестового вектора.

3) Попередня обробка зображень. Даний модуль дозволяє готувати зображення для подальшої їх обробки. Так, є методи завантаження зображень у форматі *PNG* і *PGM*. Модуль дозволяє привести зображення розмірностей великих, ніж 92×112 до даним параметрам, з тією умовою, що особи на зображенні розташоване точно по центру.

Є функція завантаження кольорових *PNG* зображень з приведенням їх до формату відтінків сірого.

3.2.2. Модуль ідентифікації по голосу

В основі даного модуля лежить алгоритм обчислення крейда-частотних кепстральних коефіцієнтів з аудіозапису, кластеризації та обчислення відстаней до вектора тестового сигналу. Також даний модуль відповідає за завантаження звукових файлів у форматах *WAV* з частотою дискретизації 16 *KHz* і 16 біт на вимір.

Навчання проводиться при додаванні нової людини в базу. У такому випадку кожен обраний аудіофайл розбивається на вікна довжиною 30 *мс*, для кожного вікна розраховуються крейда-частотні кепстральних коефіцієнти, формується новий кластер, відповідний цій людині, для цього кластера обчислюється вектор-центр ваги, що характеризує мова даної людини.

На етапі ідентифікації також проводиться кадрування сигналу, для кожного кадру розраховуються коефіцієнти, розраховується вектор-центр ваги тестового сигналу. Після чого обчислюються квадрати Евклідових відстаней від тестового вектора до кожного вектора навчальної вибірки. Відстань зводиться в квадрат для отримання більш точних результатів ідентифікації – відстані до тих кластерів, до яких не відноситься тестовий вектор, стає істотно більшим у порівнянні з відстанню до кластера, до якого цей сигнал належить.

Емпірично на основі 40 експериментів було визначено порогове значення відстані ідентифікації було встановлено рівним 5.

Кожен сигнал при підготовці до вилучення крейда-частотних кепстральних коефіцієнтів проходить етап попередньої обробки, на якому статистично обчислюються і видаляються ділянки тиші.

Модуль ідентифікації по голосу для завантаження аудіофайлу використовує додаткову функцію, яка дозволяє завантажувати аудіофайли у форматі *WAV* (16 *KHz*, 16 біт на семпл). Функція також перевіряє відповідність файлу даними параметрами, зчитуючи інформацію про кодування з заголовка файлу.

3.2.3 Модуль зберігання даних і інтерпретації результатів

Даний модуль відповідає за зберігання навчальних даних для кожної людини, організовує взаємодію між графічним інтерфейсом і модулями ідентифікації, інтерпретує і об’єднує результати ідентифікації по обом факторам.

При додаванні нової людини в вибірку відбувається отримання вхідних даних від графічного інтерфейсу: вибрані звукові файли і зображення або дані отримані з мікрофона і веб-камери, ім’я нового людини. Дані передаються в модулі ідентифікації, де з них виділяються вектора особливостей, зберігаються в пам’ять. Для подальшої роботи самі файли, за винятком одного зображення, не потрібні, на увазі економії системних ресурсів. Кожна людина представляється набором векторів зображень його особи, векторами крейда-кепстральних частотних коефіцієнтів і одним зображенням його особи для наочного відображення результату ідентифікації.

Для ідентифікації проводиться аналогічна завантаження зображення і даних голосу.

Завантажується матриця навчальної вибірки зображень і разом з тестовим вектором передається в модуль ідентифікації по зображенню, де відбувається ідентифікація.

Збираються вектора-центроїди голосу з усіх кластерам, передаються разом з тестовим вектором в модуль ідентифікації по голосу.

На виході обох модулів ідентифікації є дані про індекс і видаленні найбільш близького вектора зображення і найбільш близького вектора звуку. Дані результати об'єднуються в такий спосіб:

А) якщо результат ідентифікації по зображенню вище порогового, а результат ідентифікації по голосу – нижче, то повертається результат ідентифікації по голосу;

Б) якщо результат ідентифікації по голосу вище порогового, а результат ідентифікації по зображенню – нижче, то повертається результат ідентифікації по зображенню;

В) якщо обидва результату вказують на одну людину, то повертається загальний результат;

Г) якщо обидва результату нижче порогового, але вказують на різних людей, то повертається результат негативної ідентифікації;

Д) якщо обидва результату вище порогового і вказують на різних людей, то повертається результат негативної ідентифікації.

3.3. Описання відкритих бібліотек для реалізації алгоритму *Fisherface*

Даний алгоритм є розширенням алгоритму *Eigenface*. Відмінністю є кластеризація навчальних векторів, для чого розраховуються всередині-класові і між-класові коваріаційні матриці [1].

$$S_b = \sum_{i=1}^{c} \sum_{x \in X_i} (x - m_i)(x - m_i)^T,$$

де c – кількість класів у вибірці, вектор, що належить класу,-середній вектор i-го класу $xX_i m_i$

$$S_b = \sum_{i=1}^{c} N_i (m_i - m)(m_i - m)^T,$$

де c – кількість класів,

N_i- кількість елементів в i-тому класі,

m_i- середній вектор i-го класу,

m- середній вектор всієї вибірки.

Наступним кроком розраховується матриця головних компонент:

$$W_{PCA} = \arg max_W W^T S_T W,$$

де W – вектор тестового зображення,

S_T – ковариационная матриця.

Завершальним кроком є розрахунок підсумкової матриці:

$$W_{PCA} = \arg max_W \frac{|W^T W_{PCA}^T S_b W_{PCA} W|}{|W^T W_{PCA}^T S_w W_{PCA} W|}.$$

3.3.1. Переваги і недоліки відкритої бібліотеки *DLIB*

Переваги: *Open source* рішення, можна брати участь в розвитку і дивитися поточні тренди.- Написана на C ++. Має підтримку для *iOS* у вигляді *cocoapods*: *pod* '*dlib*' .- Можна також інтегрувати в вигляді *C* ++ бібліотеки. Працює на *Windows, Linux, MacOS*. Працювати можна і в *swift* додатках, написавши обгортку на *objective-c* ++.

Недоліки: Великий розмір підключається бібліотеки. 40 мегабайт в вигляді *pod*.- Високий поріг входу. Велика кількість внутрішніх алгоритмів, під кожен з яких має бути писати обгортку на *Objective-C*.

3.3.2. Переваги і недоліки відкритої бібліотеки *OpenCV* (*Open Source Computer Vision Library*)

Переваги: Найбільше ком'юніті, регулярно бере участь в поддержке.- Написана на C ++. Має підтримку для *iOS* у вигляді *cocoapods*: *pod* '*OpenCV*'.

Недоліки: Високий поріг входа.- Великий розмір підключається бібліотеки. 77 мегабайт в вигляді *pod*, 180 мегабайт у вигляді *C* ++ бібліотеки (рис. 3.2).

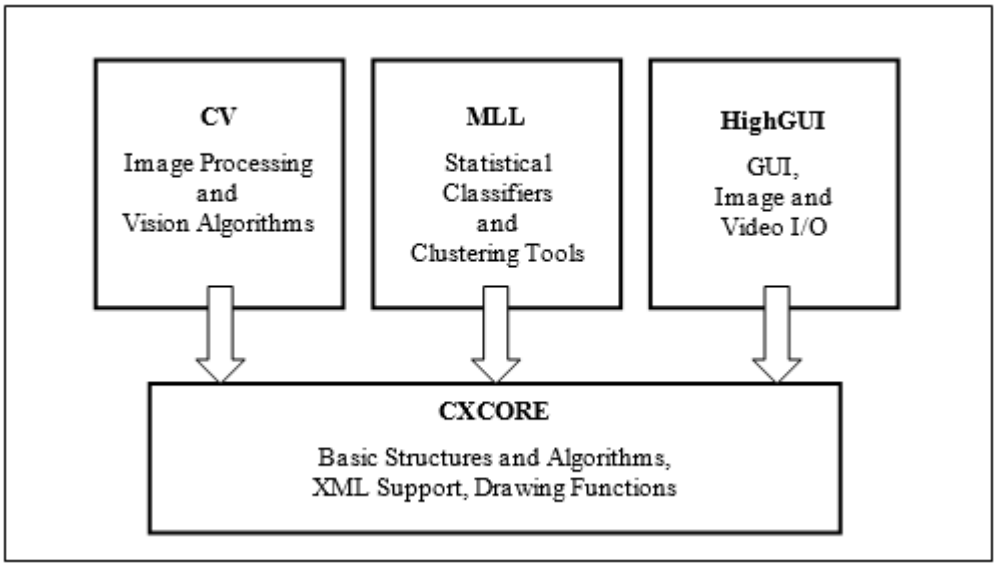

Рис. 3.2. Компоненти бібліотеки *OpenCV*

3.3.3. Переваги і недоліки відкритої бібліотеки *iOS Vision Framework*

Переваги: Проста інтеграція в пріложеніе. Містить зручний конвертер, який підтримує кілька різних моделей інших фреймворків (*Keras, Caffe, scikit-learn*). Коробкове рішення з малим размером. Працює на *GPU* (рис. 3.3).

Недоліки: є частиною *CoreML*, тому підтримує лімітовану кількість типів моделей інших існуючих фреймворков.- Немає підтримки *TensorFlow*, одного з найпопулярніших рішень машинного навчання. Доведеться витратити багато часу на самописние конвертери.- Є високорівневою абстракцією. Вся імплементація закрита, звідси неможливість контроля.- *iOS* 11+.

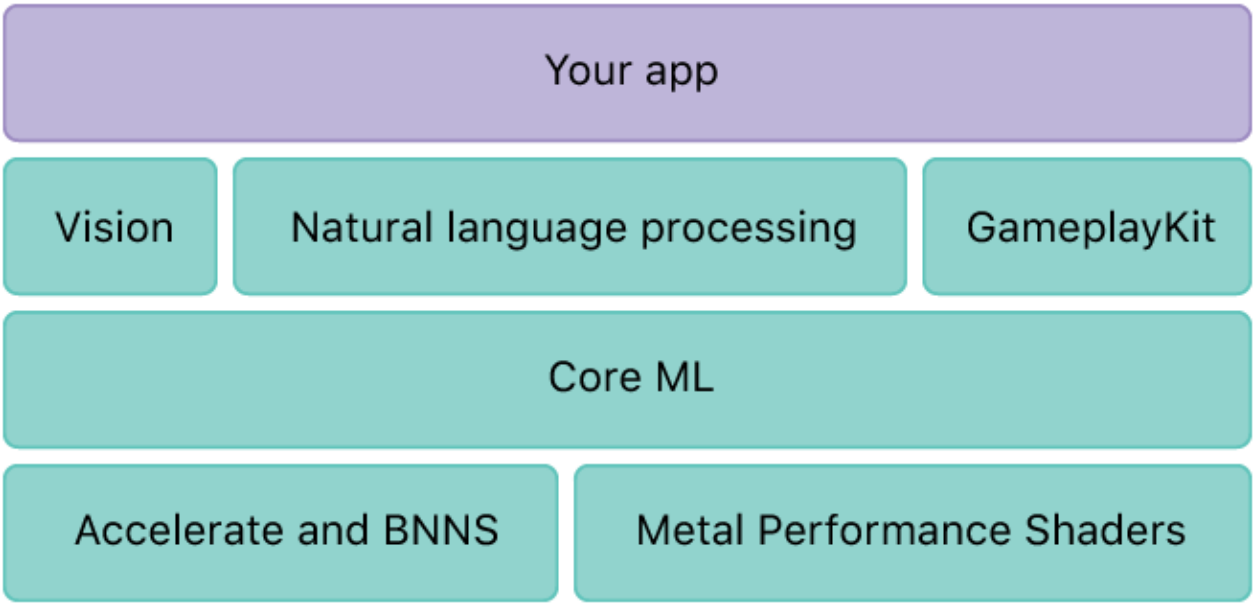

Рис. 3.3. Структура *CoreML*

3.4. Оцінка ефективності систем ідентифікації по геометрії особи

Найчастіше на рівні кінцевого користувача необхідно детально оцінити ефективність впровадження і використання біометричної системи в конкретних умовах (певна модель і розташування відеокамери, освітленість приміщення з комп'ютером і ін.). Це буває необхідно і для «великих» систем, і для засобів біометричного контролю використання комп'ютерів, доступних пересічним користувачам в побуті.

Ефективність – це властивість системи, що характеризує її здатність виконувати поставлене відповідно до її призначення завдання в певних умовах і з певною якістю, тобто ступінь пристосованість системи до виконання поставлених перед нею завдань. Визначення ефективності системи необхідно для порівняння різних систем одного призначення.

Виходячи з викладеного, стосовно біометричних систем ідентифікації, ефективність – це здатність систем достовірно встановлювати особу людини, яка є суб'єктом ідентифікації. Очевидно, що практично це відповідає використовуваному повсюдно поняттю «надійність біометричної системи».

Однак, оскільки біометричні системи не є стендовими, а використовуються на практиці для вирішення користувачами реальних завдань, слід не просто розглядати їх технічна досконаліть, але ще й аналізувати всі фактори, важливі кінцевого споживача, виключивши в той же час ті, вплив яких на практичну сторону питання не принципово. Тобто замість чисто технічної оцінки ефективності систем слід аналізувати їх сукупну споживчу ефективність. При такій інтерпретації доцільно спільно розглядати три складові – технічну, економічну і емпіричну, – і оцінювати сукупну ефективність не тільки оптимальністю технічних величин, але і зіставленням економічних показників і оцінок користувачів. Для аналізу можуть бути використані загальновживані методи,

Якщо розглядати прикладні системи більш широко (з урахуванням цільового призначення), необхідно враховувати вплив підсистем, супутніх біометричних засобів. Наприклад, надійність системи обмеження фізичного доступу прямо залежить не тільки від надійності біометричних сканерів, але і від елементарної міцності замикається нею замку, а системи контролю доступу до комп'ютера – також від можливості альтернативної аутентифікації сторонньої особи тільки по вкраденому паролю. Далі буде розглядатися ефективність саме біометричних засобів, що входять в прикладні системи у вигляді окремих підсистем або функціональних елементів.

Визначення ефективності має сенс тільки стосовно до конкретного об'єкта, специфіка якого і визначає застосовуваний для цього підхід і методи. Оскільки в останні роки біометричні системи масово використовуються в системах безпеки організацій – суб'єктів малого та середнього бізнесу, а також приватними особами, далі будемо розглядати саме цю широко затребувану сферу їх застосування. Очевидно, що типовим об'єктом подібного роду є невелике приміщення (будинок, магазин, офіс організації) з декількома персональними комп'ютерами (комп'ютеризованими робочими місцями). Для визначеності домовимося, що використовується, наприклад, три комп'ютери. Подібний об'єкт в силу очевидних обставин відноситься максимум до середнього класу захищеності, що передбачає, в першу чергу,

Раніше було показано (див. Розділ 1), що найбільш підходящими тут є рішення, засновані лише на декількох біометричних технологіях: ідентифікація за відбитками пальців, за формою обличчя і голосу. Системи з ідентифікацією за формою особи в подібній ситуації більш кращі, що також обумовлено раніше (див. Розділ 2), і можуть являти собою як систему обмеження доступу в приміщення, так і систему контролю доступу до комп'ютера (в разі, якщо критичним є саме несанкціоноване використання комп'ютерів).

Дослідження ефективності в самих різних областях ведуться давно. Проте, зараз можна говорити про більш-менш коректних локальних рішеннях, але поки що не йдеться про будь-якому загальному системному відповіді. Замість теоретично чітко визначеного сімейства рішень є тільки багатий набір всіляких підходів, концепцій, точок зору і т.д.

Вибір конкретних методів оцінки ефективності індивідуальний для кожного випадку і визначається в основному тією областю, до якої належить дана система (соціально-економічна, екологічна, енергетична ефективність, ефективність менеджменту, системи зв'язку, способу переробки нафти і т.д.). При цьому використовуються найрізноманітніші дослідні прийоми і інструменти, а отримані результати інтерпретуються із застосуванням методів, запозичених з різних дисциплін – економіки, соціології, психології. Саме цим і викликана необхідність обов'язкового уточнення тієї області, в якій проводиться оцінка ефективності.

Порівняльна оцінка ефективності біометричної технології, як і будь-якого іншого проекту, необхідна, в кінцевому рахунку, для виявлення найбільш кращою альтернативи, дозволяючи робити вибір на користь оптимального рішення. Так як пошук найбільш ефективного біометричного рішення по суті є завданням оптимізації, можна використовувати два концептуально різних підходи.

Перший підхід являє досліджуваний об'єкт (в даному випадку цільову систему для впровадження біометрії) в якості «чорного ящика» і не виробляє аналізу внутрішніх процесів об'єкта. Він статистично встановлює кореляційні зв'язки між вхідними (керованими) об'єкта та вихідними параметрами, в якості

яких виступають показники якості і ефективності. Головною перевагою цього підходу є його спільність і можливість застосування для всіх випадків оптимізації. Однак для кожного конкретного випадку при цьому потрібне проведення статистичного дослідження за індивідуальним планом (наприклад, повно-факторний експеримент), результати якого стануть непридатними при зміні характеристик досліджуваної системи.

Другий підхід заснований на моделюванні системи і передбачає розробку і використання спеціальних критеріїв оптимальності – характерних показників рішення задачі оптимізації, за значенням яких оцінюється ступінь відповідності поставленим вимогам, тобто оптимальність рішення. Оптимальний результат при цьому досягається при підтримці оптимальних значень цих критеріїв (мінімальність критерію або ж, навпаки, максимальна його величина) шляхом зміни вхідних параметрів, що є, по суті, управлінням за непрямими вимірами. В одному завданню може бути встановлено безліч критеріїв оптимальності, загального методу для їх вибору не знайдено і при виборі, в основному, керуються досвідом або певними рекомендаціями. Хоча в задачах оптимізації в різних галузях використовуються абсолютно різні величини, існує ряд універсальних критеріїв, які можна застосувати практично повсюдно через їх фундаментального значення. Наприклад, основні економічні показники (собівартість, питома ресурсомісткість) можуть оцінювати абсолютно будь-яку матеріальну систему, а обчислювальна складність – будь-яку алгоритмічну модель.

Так як в даному випадку при аналізі біометричної системи не представляється можливим проведення скільки-небудь значних статистичних досліджень, для вибору оптимального рішення далі буде використовуватися другий підхід. При цьому, в силу специфіки завдання, в якості критеріїв оптимізації будуть розглядатися не змодельовані функціонали, а безпосередньо самі параметри системи, які явно визначають кінцеву якість і ефективність. Значення таких характерних показників можуть бути легко змінені в ході рішення, не вимагаючи проміжних обчислень. Таким чином, створення

адекватної моделі системи замінюється логічними міркуваннями, суб'єктивними припущеннями і перебором відомих варіантів.

Як було показано вище, сукупна споживча ефективність роботи біометричної системи характеризується показниками ефективності – параметрами системи, які об'єктивно і є критеріями оптимальності.

Очевидно, що весь обсяг показників, що характеризують ефективність, може бути розділений на декілька груп, які об'єднують схожі за змістом параметри. В даному випадку виділимо наступні групи показників ефективності систем:

– результативність (практично це – технічна ефективність, надійність ідентифікації, яка визначається низкою технічних показників системи);

– оперативність (сукупність характеристик, що визначають, в кінцевому рахунку, швидкість і зручність – ефективність – використання системи);

– ресурсомісткість (сукупність характеристик, що визначають витрати на впровадження і зміст системи, тобто її економічну ефективність).

Далі розглянемо окремо ці групи факторів і визначимо показники, що впливають на ефективність біометричної системи ідентифікації по геометрії особи, які в подальшому будуть використані як критерії оптимальності при порівняльній оцінці ефективності.

Технічні показники ефективності, як було показано вище, характеризують собою надійність біометричної системи, яка описується за допомогою методів математичної статистики, так як метод біометричного контролю має імовірнісну природу, а в основі будь-якої біометрії лежить статистика (див. Розділ 1).

При скануванні система (пристрій) порівнює дані користувача з еталоном і видає відповідь «збігається – не збігається». Процедура аутентифікація з математичної точки зору є перевіркою статистичної гіпотези, при якій можливі помилкові висновки двох типів: відкидання гіпотези в разі, коли вона насправді вірна (помилковий відмова в доступі легальному користувачеві, «помилкова тривога») і прийняття гіпотези, якщо вона на насправді невірна (помилковий допуск стороннього, «пропуск цілі»). Ці події названі відповідно «помилкою першого роду» і «помилкою другого роду».

Ймовірності цих помилок в термінах біометрії позначаються коефіцієнтами – *FAR* (*False Acceptance Rate*) і *FRR* (*False Rejection Rate*). Зазвичай передбачається нормальний розподіл ймовірності. Значення *FAR* і *FRR* можуть бути виражені як у вигляді безрозмірних коефіцієнтів (0.00-1.00), так і в процентному відношенні.

Величина *FAR* практично характеризує ймовірність збігу біометричних характеристик двох людей, по ній також можна зробити непрямий висновок про схильності системи «злому». Величина *FRR* визначає мінімальну якість і кількість даних, що надаються системою для нормальної ідентифікації людини.

Так як ні одна система на сьогодні не здатна гарантувати повну відсутність помилок, ймовірність хибнопозитивної і помилково негативні ідентифікації набувають найбільше практичне значення для оцінки якості біометричної системи.

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 неуповноважених осіб за будь-яких обставин, як більш критичного обставини. Очевидно, що для цього необхідний дуже низький *FRR*, навіть на шкоду величиною *FAR*.

Імовірність помилки (*FRR* і *FAR*) сильно залежить і від особистості суб'єкта аутентифікації і може бути визначена персонально для кожної людини, хоча очевидно, що одну людину недостатньо для висновку про надійності біометричного рішення в цілому. У зв'язку з цим за аналогією згадується також «помилка третього роду», коли ідентифікація неможлива через відсутність або значного пошкодження у людини індивідуальних ознак, що застосовуються в алгоритмі (травма, ампутація, шрами). Імовірність подібної помилки – *FER* (*Failure to Enroll Rate*) – показує відсоток людей, які не можуть завершити реєстрацію в системі. Такі невдачі можуть бути пов'язані з недостатньою підготовкою, екологічними, ергономічними умовами, які роблять біометричний фактор просто непридатним для певних людей. Не можна забувати,

Помилки першого і другого роду не підлягають ремонту принципово і мова може йти тільки про те, щоб знизити їх ймовірність до практично прийнятних величин. Оскільки статистика помилок визначається методикою і тривалістю тестування, об'ємом і характером статистичних вибірок, ймовірності помилок є не тільки функцією надійності методу (статистично обґрунтована ймовірність збігу характеристик у різних людей), але і цілого ряду умов експлуатації. Зазвичай характеристики алгоритму даються для якоїсь «ідеальної» бази, або просто для добре підходить, де викинуті нерізкі і змащені кадри. Сканери (точність зчитування необхідного обсягу інформації) також дуже сильно впливають на отриману статистику *FAR* і *FRR*. В реальних умовах ці цифри можуть змінюватися в десятки разів.

На практиці ймовірність помилок першого і другого роду у систем біометричної аутентифікації може бути набагато вище, розрізняючи в широких межах від реалізації до реалізації, незважаючи на зусилля, прикладені для їх зниження. Тому для спрощення використання сучасні біометричні рішення мають настройки чутливості, даючи можливість підбирати оптимальний для кожного випадку співвідношення точності ідентифікації та зручності використання. При цьому система використовує настроюється порогове значення вірогідності, що визначає, наскільки точно дані користувача повинні відповідати наявній зареєстрованому еталону. Змінюючи чутливість, на практиці можна задавати значення *FAR* і *FRR*.

Для систем ідентифікації по контурах особи характерне значення *FAR* – 0,1%, а *FRR* становить кілька відсотків, що для сучасних систем безпеки досить посередньо.

Для ряду алгоритмів (3*D* розпізнавання) заявлені *FRR* = 0,1% при аналогічному *FAR*, але бази, за якими вони отримані, чи не репрезентативні (вирізаний фон, однакове вираз обличчя, однакові зачіска, освітлення).

Як видно, статистичні показники методу досить скромні, що обов'язково повинно бути враховано на практиці. Так, стосовно до системи аутентифікації для контролю доступу на об'єкт середнього ступеня захищеності, слід зазначити наступне. Необхідно встановлювати максимальну чутливість алгоритму для

зниження *FRR*, з часом дещо знижуючи її в разі занадто частих помилкових відмов доступу, або організувати стандартні умови для перевірки: розташування камери, навчання співробітників, хороше освітлення контрольної зони. У невеликій організації з кількістю працівників не більше 30, система розпізнання особи очікувано може видавати одну-дві помилки відмови доступу на добу, що цілком прийнятно.

Швидкодію системи визначається часом, що витрачається системою на ідентифікацію користувача. Це час набуває тим більшої значущості, чим більша кількість процедур ідентифікації потрібно зробити за певний період. Наприклад, п’ять секунд – трохи при разовому тестуванні, але якщо сотні людей на прохідній будуть проходити його кілька разів в день, сукупна втрата часу буде значною.

Однак не тільки технічним швидкодією визначається якість біометричної системи. Важливі також деякі емпіричні показники, які характеризують суб’єктивну оцінку роботи системи користувачами і визначають швидкість роботи системи як функцію зручності її використання. Розглянемо далі найбільш очевидні і значущі з таких показників.

Простота використання системи характеризує, наскільки складно скористатися біометричним сканером, чи можлива ідентифікація «на ходу». Визначає головним чином, чи достатньо коректно обрана система стосовно соціальних особливостей об’єкта. Наприклад, при контролі доступу в офіс, на початку робочого дня можливі черги в зоні аутентифікації, якщо співробітники приходять на роботу одночасно, а складність аутентифікації висока. Розпізнавання обличчя особливо зручно через відсутність фізичного контакту і ідентифікації людини без його участі, камерою зовнішнього виявлення (хоча можливо це лише при малій кількості суб’єктів в базі і невеликому потоці людей, що знімаються камерою).

Сумісність з існуючими системами – це можливість вбудувати біометричні засоби в уже існуючу інфраструктуру. Розглядаючи конкретну систему контролю доступу до комп’ютерів, потрібно переконатися в коректності її роботи з наявним обладнанням і ПЗ, а також проаналізувати можливість її інтеграції в уже

встановлені системи захисту. Конфлікти в роботі підсистем неминуче відіб'ються на сукупному швидкодії.

Кількісну оцінку таких показників в задачі оптимізації виробляють за умовними безрозмірним шкалами – кожному з альтернативних варіантів привласнюють свою оцінку в балах. Найвища оцінка, очевидно повинна відповідати найкращому значенню показника.

Для подібної кількісної оцінки неісчісляемих характеристик і властивостей може застосовуватися метод експертних оцінок. Експертне оцінювання – це процедура отримання будь-якої оцінки на підставі думки фахівців (експертів) з метою подальшого прийняття рішення. Експертне оцінювання особливо важливо при вирішенні задач, які чинять спротив рішенню звичайним аналітичним способом (наприклад, вибір найкращого серед наявних варіантів вирішення, прогнозування розвитку процесу, пошук вирішення складних завдань).

Ефективність методу і правильність отриманих рішень безпосередньо визначається вибором експертів для формування експертних груп. Кількість членів експертної групи значно менше в порівнянні з кількістю респондентів, опитуваних при масовому опитуванні. Однак при цьому інформація, отримана при експертному опитуванні, як правило, є досить достовірною і надійною, оскільки респондентами є висококваліфіковані в даній області фахівці.

Експертне опитування проводиться у формі інтерв'ю або у вигляді анкетування. В ході опитування перед експертом ставлять питання, відповіді на які значимі для досягнення програмних цілей. При цьому передбачається індивідуальне заповнення експертом розробленого формуляра-запитальника, за результатами якого проводиться всебічний аналіз проблемної ситуації і виявляються можливі шляхи її вирішення. Велике значення має правильне формулювання питань в опитувальнику, що дозволяє визначитися зі ставленням експерта щодо кожного питання у вигляді кількісної оцінки, а також можливість узгодження оцінок, отриманих від різних експертів. Для отримання коректних оцінок слід, по можливості, усувати взаємовплив експертів і зменшувати вплив сторонніх чинників.

Використовується дві техніки проведення експертного опитування: індивідуальне опитування (заснований на думці окремих експертів, незалежних один від одного) і колективний опитування (заснований на використанні колективної думки групи експертів). Спільне думку володіє більшою точністю, ніж індивідуальна оцінка кожного з фахівців. Для проведення колективних експертних опитувань використовують метод Дельфі (Дельфийская техніка), мозковий штурм і метод аналізу ієрархій.

Існує чимало способів формування експертних оцінок: метод асоціацій (порівняння зі схожим за властивостями об'єктом), метод парних порівнянь (попарне зіставлення альтернативних варіантів), метод векторів переваг (аналіз всього набору альтернативних варіантів і вибір найбільш бажаних), метод фокальних об'єктів (заснований на перенесенні ознак випадково відібраних аналогів на досліджуваний об'єкт) і ін.

Найбільш обгрунтований з позицій математичної статистики метод парних порівнянь, що передбачає порівняння експертами безлічі пар, складених з альтернативних варіантів. Для кожної пари вибирається найкращий варіант, відповідь вказується дворівневої оцінкою в уніфікованій формі, а потім сукупність відповідей обробляється статистично. Основною перевагою тут є те, що для бінарних порівнянь (на відміну від порівняння декількох варіантів) є добре пророблений статистичний апарат, що дозволяє визначати достовірність оцінок, представництво вибірки і однорідність масиву оцінок.

Економічна складова характеризується витратами і отриманим економічним ефектом. У фінансовому аналізі можна використовувати кілька методів: прямий розрахунок економічного ефекту, порівняння фінансового стану до і після заходу, оцінка рентабельності, метод цільових альтернатив (зіставлення планованих показників з досягнутими).

Очевидно, що ефект для користувачів першого рівня зводиться до зниження втрачених людино-годин, до скорочення експлуатаційних витрат, а також підвищення продуктивності праці. Оскільки при впровадженні системи аутентифікації економічний результат не може бути визначений негайно, або його взагалі можна тільки припустити, доцільніше на практиці оцінити

економічну ефективність від застосування біометричного кошти через суму витрат на впровадження і зміст системи. Досліджуваним матеріалом є фінансові (бухгалтерські) дані.

Витрати на впровадження – очевидна грошова сума. Крім вартості системи, до цієї ж статті витрат відноситься і навчання персоналу, витрати на доставку і установку і т.п.

Витрати на утримання системи визначаються рівнем її технічного виконання і мають на увазі витрати на електроенергію, зарплату обслуговуючого персоналу, ремонт і т.д.

Визначення ефективності аналізованих рішень здійснюється при цьому за допомогою критерію мінімуму сукупних витрат: чим менше витрати при рівних характеристиках системи, тим більш оптимальним є рішення.

Що стосується аналізованої системі аутентифікації слід зазначити таке. Для аутентифікації користувачів цілком реально використовувати наявне обладнання, наприклад, підключити сервер аутентифікації до камери спостереження. При цьому усувається необхідність покупки додаткового устаткування, що дозволяє мінімізувати витрати, обмежуючись придбанням тільки відповідного програмного забезпечення.

Оскільки вибрані параметри згруповані за категоріями, які, в свою чергу, є складовими загальної споживчої ефективності, оцінка якої і потрібно для визначення оптимального рішення, можна уявити взаємозв’язок і вплив параметрів на підсумковий результат у вигляді ієрархічної структури.

Дані параметри безпосередньо виступають в ролі критеріїв оптимальності при оптимізації ефективності біометричної системи.

Для проведення порівняльного аналізу ефективності біометричних систем необхідно скласти максимально розгорнутий перелік альтернативних варіантів вирішення проблеми, для яких можливе визначення перерахованих вище показників. Наприклад, в даному випадку можна запропонувати наступні варіанти біометричних рішень:

– система обмеження фізичного доступу в приміщення з комп'ютерами, що використовує камеру зовнішнього спостереження і стандартну домофонну систему, керовану з сервера аутентифікації в контрольованому приміщенні;

– аналогічна система, але що використовує спеціальний біометричний сканер, встановлений в контрольній зоні;

– система обмеження використання комп'ютерів, заснована на використанні камер, підключених до кожного комп'ютера, і програмного забезпечення на цих комп'ютерах (на зразок «*Rohos Face Logon*»), що виробляє аутентифікацію для входу в операційну систему;

– аналогічна система, але з перехресної біометричної аутентифікації, яка виробляє послідовну перевірку користувача по обличчю двома різними методами (наприклад, за унікальними характеристиками і методом «*Eigenface*», розглянутим раніше), що вимагає наявності двох програм аутентифікації.

Як було показано вище, технічні показники роботи систем на практиці можуть значно відрізнятися від значень, заявлених виробником. Однак при оцінці ефективності за основу треба брати саме середні заявлені значення, так як реальні до впровадження конкретного рішення передбачити неможливо. В даному випадку необхідні показники приймемо за даними, декларованим провідними виробниками.

Фінансові показники, відібрані раніше для аналізу ефективності, є прості грошові суми і можуть бути легко розраховані, виходячи з переліку необхідного обладнання кожного запропонованого варіанту. Ціни на обладнання та програмне забезпечення можна прийняти на підставі цін провідних постачальників (офіційних українських дилерів), зазначених у прайс-листах, доступних в мережі Інтернет. Вартість доставки і монтажу приймемо пропорційною вартості обладнання з коефіцієнтом 0,4. Середньорічну вартість експлуатації також приймемо, виходячи з технічної оснащеності пропонованих до впровадження систем: 25-30% від вартості нового обладнання (для перших трьох років). Значення множників обрані, виходячи з відомих у фінансовому аналізі даних щодо впровадження електронних систем в промисловості.

Стосовно до біометричних систем розпізнавання особи, оцінки неісчісляемих показників можуть бути отримані шляхом експертного опитування компетентних технічних фахівців, фахівців з продажу, знайомих зі статистикою впровадження, а також користувачів, які мають досвід використання систем в подібних умовах. Необхідні дані візьмемо з опублікованих оглядів [3, 8], вважаючи їх досить адекватними і надійними.

Очевидно, що наведені дані є орієнтовними, і будуть змінюватися в процесі експлуатації (наприклад, через зношування основних фондів буде збільшуватися вартість експлуатації і погіршуватися надійність).

Крім кількісної оцінки варіантів по кожному з критеріїв, потрібно визначити пріоритет критеріїв, так як деякі з них більш важливі при виборі, а деякі – менш. Для ранжирування параметрів вони розподіляються за рівнями значущості для кожного варіанта рішення. Пріоритети (ваги) кожного з n критеріїв представляються в діапазоні від 0 до 1 наступним чином:

$$0 < p_i < 1,\ i = 1 \ldots n;$$
$$p_1 + \ldots + p_n = 1$$

Пріоритет критеріїв встановлюється при аналізі альтернатив суб'єктивно, виходячи з важливості їх в конкретних умовах. Висновки про важливість критеріїв повинні бути обгрунтовані, інакше результати, по суті, будуть спочатку не валідними. Потрібно відзначити, що якщо параметри різні і не компенсують один одного, розставити пріоритети критеріїв відповідним чином особливо важливо. Так, для системи аутентифікації, завдання якої – контроль доступу, найважливішим є показник *FRR*, тоді як вартість має дещо менше значення, превалируя, в свою чергу, над швидкістю аутентифікації.

Приймемо для даного випадку пріоритет критерію *FRR* системи найвищим (наприклад 0,95), для *FAR* – трохи менше (0,85), далі – витрати на впровадження (0,7), зручність використання (0,5) і т.д . У відповідності до розділу (3.1) далі наведемо ці значення до пайової висловом.

Оцінки за різними критеріями можуть мати різні шкали (наприклад, *FRR* виражається у відсотках, а вартість впровадження – в рублях). Для можливості спільного використання різнорідних параметрів при згортку необхідно попередньо провести їх нормування, тобто привести їх у безрозмірну форму в однаковому діапазоні, зазвичай від 0 до 1. При цьому для кожного варіанта X оцінки по *n* критеріям виражаються так:

$$0 \le f_i(x) \le 1,\ i = 1 \ldots n.$$

Крім приведення до загального вигляду нормировка дозволяє зробити однозначний градуювання шкали, за якою визначається оптимальність значення кожного конкретного параметра ефективності. Це необхідно тому, що в залежності від сенсу використовуваного критерію оптимальний результат досягається або при мінімальності критерію, або, навпаки, при максимальній його величині. Необхідність максимізувати або мінімізувати критерій і визначає діапазон нормованої шкали.

У даній роботі використовується метод нормування параметрів за еталонною шкалою: для кожного параметра, виходячи з його фізичного сенсу і конкретних значень, встановлюється мінімальне f_{min} і максимальне f_{max} значення показника в натуральному вираженні. При цьому нормовані значення розраховуються для негативних і позитивних критеріїв відповідно так:

$$f_{\text{негат}} = \frac{f_{\text{вимір}} - f_{min}}{f_{max} - f_{min}};$$

$$f_{\text{позит}} = \frac{f_{max} - f_{\text{вимір}}}{f_{max} - f_{min}}.$$

В даному випадку для всіх нормованих показників з табл. 3.2 встановлюється діапазон від 0 до 1. На підставі змісту окремих показників, при цьому висуваються вимоги мінімальності всіх критеріїв, крім величин

стабільності роботи і простоти використання, для яких потрібно максимальність критерію.

Вибір еталонної шкали для параметрів проводиться на підставі їх значень і одиниць вимірювання. Наприклад, емпіричні оцінки зроблені за десятибальною шкалою [3, 8], тому еталонна шкала для них 0 – 10 балів. У той же час, виходячи з практичних міркувань придатності системи, процентні значення *FRR* і *FAR* не можуть бути більше 10% і 0,05% відповідно.

При пошуку оптимального рішення в багатокритеріальних задачах з різнорідними показниками велике значення має теорія прийняття рішень, методи якої дозволяють однаково працювати як з технічними, так і з економічними показниками, дозволяючи підключати статистику і фінансовий аналіз.

Якщо потрібно прийняти якесь рішення, вибравши один з можливих варіантів як оптимальний, і при цьому є кілька критеріїв ефективності рішення, мова йде про рішення багатокритеріальної задачі. Зазвичай кожен з варіантів вирішення багатофакторної завдання превалює по одним критеріям, програючи по іншим. Основним способом вирішення в цьому випадку є зведення задачі до однокритерійним за допомогою «згортки» критеріїв в один комплексний критерій, тобто сукупне уявлення кількох критеріальних оцінок у вигляді єдиної оцінки, званої цільової функцією (функцією корисності).

3.4.1. Тестування модуля ідентифікації за зображенням особи

Об’єкт тестування – модуль ідентифікації по зображенню особи.

Вхідні дані – відкрита вибірка осіб *Cambridge University Computer Laboratory*, «*The Database of Faces*» (источн).

Дана вибірка містить по 10 зображень для 50 осіб в форматі *PGM* (92 × 112 Пікслей).

Навчальна вибірка:

40 осіб;

3 зображення на людину.

Тестова вибірка:

40 осіб;

3 зображення на людину – 120 тестів.

Результати ідентифікації:

93 успішних ідентифікацій;

12 невірно ідентифіковано (нижче порогового значення)

15 невірно ідентифіковано (вище порогового значення)

77,5% точність ідентифікації.

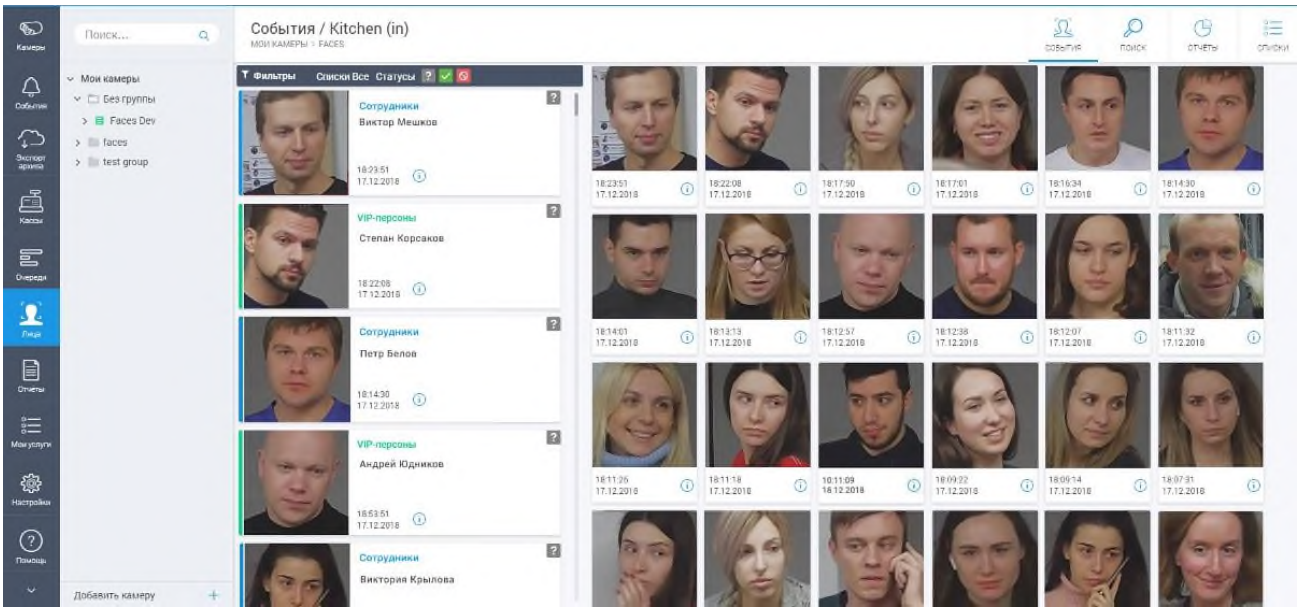

Рис. 3.4. Реалізація системи ідентифікації особистості за зображенням особи

3.4.2. Тестування модуля ідентифікації по аудіозаписи голосу

Об’єкт тестування – модуль ідентифікації по аудіозаписи голосу.

Вхідні дані вибірка записів голосів людей. Також має вільний доступ для дослідницьких цілей, являє собою набори аудіо коротких аудіозаписів (16 *KHz*, 16 біт) від різних людей.

Навчальна вибірка:

– 40 людей

– 21 секунда записи голосу

Тестова вибірка:

– 40 людей

– 12 секунд запису голосу – 40 тестів.

Результати ідентифікації:

– 33 вірно ідентифіковано

– 7 невірно ідентифіковано (нижче порогового значення)

– 82,5% вірних ідентифікацій

3.4.3 Тестування об’єднання факторів

Навчальна вибірка:

– 40 людей

– 3 зображення на людину

– 21 секунда аудіозаписи

Тестова вибірка: 40 людина

– 3 зображення на людину.

– 3 аудіозаписи по 5 секунд

– 120 тестів

Результати ідентифікації:

– 102 вірно ідентифіковано

– 18 невірно ідентифіковано (нижче порогового значення)

– 85% вірною ідентифікації.

Таблиця 3.2

Порівняння результатів

Ідентифікація	Кількість тестів	Кількість вірних ідентифікацій	Відсоток помилок
По зображенню особи	120	93	23.5%
За аудіозаписом голосу	40	33	17,5%
Двухфакторная ідентифікація	120	102	15%

3.6. Висновки до розділу

Завдання ідентифікації людини по зображенню особи і аудіозаписи голосу знаходяться серед найбільш складних завдань природних інтерфейсів машина-людина. Таким чином, розробка методик для вирішення цих завдань має високий

науковий інтерес. Крім цього, на практичній важливості біометричної ідентифікації складно переоцінити.

Проте, не кожен біометричний фактор легко доступний для отримання і обробки. Так, наприклад, отримання зображення райдужної оболонки ока вимагає камеру з високою роздільною здатністю, отримання відбитків пальців – додатковий пристрій для отримання зразків. У свою чергу, фотокартку особи і запис голосу можна отримати за допомогою стандартного устаткування, що є практично у кожного користувача ПК.

У процесі роботи були проаналізовані різні підходи до ідентифікації людини по обличчю і голосу, прийнято рішення про методи реалізації, розроблені способи об’єднання результатів, реалізована сама система, яка не поступається за точністю аналогічним розробкам інших дослідників.

ВИСНОВКИ

У самих різних сферах діяльності завжди були завдання, де необхідно впізнання конкретної людини. Найбільш часто це необхідно при управлінні, забезпеченні безпеки, для контролю над діяльністю людей.

В останні десятиліття для встановлення особи використовуються все більш високотехнологічні способи, найбільш затребуваним з них є біометричний розпізнавання особистості, коли людина сама є ключем, надаючи для перевірки свої унікальні фізичні або поведінкові характеристики. Область використання подібного роду засобів і систем надзвичайно розширилася в порівнянні з початковою: ідентифікація використовується не тільки в традиційних завданнях безпеки і контролю доступу, але і, наприклад, в системах «лояльних продажів» для індивідуального підходу до покупців.

Доведено унікальність для кожної людини багатьох ознак, починаючи від загальновідомих (на зразок відбитків пальців), до досить екзотичних (форма вушної раковини, температурна картина особи). Для ідентифікації по багатьом з цих ознак розроблені технічні засоби, є і повністю автоматичні системи виробляють біометричну перевірку особистості людини.

Практика показує, що заміна традиційних систем аутентифікації на біометричні дозволяє в будь-якому випадку значно підвищити загальну ступінь захищеності і технічної гнучкості організації за рахунок безумовних переваг цього підходу. Грамотна експлуатація та застосування відповідних засобів (наприклад, іноді потрібно перехресна біометрія) забезпечує на практиці майже 100% рівень точності ідентифікації, що в свою чергу дозволяє зробити висновки про правильність обраної системи.

Серед інших методів, які стали вже традиційними, найбільш перспективним слід визнати 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 потайливу перевірку і вимагає наявності тільки загальновживаного обладнання

(відеокамери). Сукупність цих якостей зумовила дуже швидкий розвиток цього методу, поставивши його за поширеністю в один ряд з дактилоскопічної перевіркою.

З підвищенням якості відеокамер і алгоритмів обробки відеопотоку і зображення вони вже перестали бути лімітуючим ланкою в системах розпізнавання особи. При використанні приблизно однакових відеокамер переважаюче значення на точність розпізнавання по обличчю набувають алгоритми обробки і формування біометричного образу. Розроблено досить велике число алгоритмів, що забезпечують не тільки високу швидкодію і точність визначення, але і дозволяють системі працювати в самих різних умовах (погана освітленість, наявність окулярів, бороди, різне положення голови і т.п.).

Сучасні системи розпізнавання особистості по обличчю знаходять застосування не тільки для серйозних завдань типу виявлення розшукуваних осіб в місцях масового перебування людей, а й для суто цивільних цілей, наприклад, як системи контролю доступу до персонального комп'ютера. Через широкого поширення недорогих веб-камер і розробки нових алгоритмів розпізнання особи, що дозволили істотно підвищити точність методу, контроль доступу до персональних (в тому числі і домашнім) комп'ютерів по обличчю користувача стає все більш значущим сегментом ринку біометричних технологій.

Аналіз найпоширеніших програм для побутового застосування приватними користувачами показує, що вони мають досить малу ймовірність помилок, забезпечують зручність в роботі. Слід визнати, що характеристики їх приблизно однакові і вибір їх залежить головним чином навіть не від специфіки роботи, а від особистих переваг користувача; для нових користувачів цей вибір в основному випадковий.

Таким чином, з результатів зробленого в даній роботі аналізу видно, що технічний стрибок вже відбувся – біометрія вийшла на перший план при вирішенні великого спектра завдань. З плином часу біометричні технології будуть розвиватися, витісняючи існуючі вже давно інші засоби. Причому розвиток можна очікувати не тільки кількісне, але і якісне – у вигляді

впровадження біометрії в нових областях (як, наприклад, це відбувається з голосовим управлінням) і появі все більш простих, інтуїтивно зрозумілих кінцевому користувачеві методів. Можна впевнено прогнозувати в тому числі і широке впровадження систем розпізнавання по обличчю. Практика масового впровадження, безумовно, дозволить знизити складність завдання пошуку найбільш ефективного вирішення і звести її до аналізу відгуків споживачів.

Завдання ідентифікації людини по зображенню особи і аудіозаписи голосу знаходяться серед найбільш складних завдань природних інтерфейсів машина-людина. Таким чином, розробка методик для вирішення цих завдань має високий науковий інтерес. Крім цього, на практичній важливості біометричної ідентифікації складно переоцінити.

Проте, не кожен біометричний фактор легко доступний для отримання і обробки. Так, наприклад, отримання зображення райдужної оболонки ока вимагає камеру з високою роздільною здатністю, отримання відбитків пальців – додатковий пристрій для отримання зразків. У свою чергу, фотокартку особи і запис голосу можна отримати за допомогою стандартного устаткування, що є практично у кожного користувача ПК.

У процесі роботи були проаналізовані різні підходи до ідентифікації людини по обличчю і голосу, прийнято рішення про методи реалізації, розроблені способи об’єднання результатів, реалізована сама система, яка не поступається за точністю аналогічним розробкам інших дослідників.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Belhumeur, P.* & *Hespanha, J.* & *Kriegman, D.* (1997). *Eigenfaces vs. Fisherfaces*: *Recognition Using Class Specific Linear Projection. IEEE Transactions on Pattern Analysis and Machine Intelligence,* 19(7), 711-721.

2. *Ejnarsson, M.* & *Nillson, M.* (2002). *Speech Recognition using Hidden Markov Model. Blekinge Institute of Technology.*

3. Аронов А.В. Основы биометрии: [Электронный ресурс] – *http://habrahabr.ru/blogs/infosecurity/*126144/

4. Татарченко Н.В, Тимошенко С.В. Биометрическая идентификация в системах безопасности: [Электронный ресурс] – *http://www.vidim.od.ua/ News_y*1.*aspx*? *pid*=22&*NewsID*=105

5. Прудников И.П., Голов А.В. Аутентификация пользователей *CIO,* #4/2006.: [Электронный ресурс] – *http://www.topsbi.ru/default.asp*? *trID*=1

6. Компьютерный журнал "КомпьюПресс",: [Электронный ресурс] – *http://www.compress.ru/article.aspx*? *id*=10113&*iid*=420

7. Попов М., Задорожный В. Биометрические системы безопасности: [Электронный ресурс] – *www.BRE.ru*

8. Сафронов В.В. Современные биометрические методы идентификации.: [Электронный ресурс] – *http://habrahabr.ru/blogs/infosecurity/*126144/

9. Борзенко А. Биометрические системы распознавания внешности: [Электронный ресурс] – *http://www.bytemag.ru/articles/detail.php*? *ID*=8520

10. *Face Verification using Correlation Filters Marios Savvides, Electrical and Computer Eng. Dept, Carnegie Mellon University Pittsburgh, PA* 15213, *U.S.A. http://www.ece.cmu.edu/~kumar/Biometrics_AutoID.pdf*

11. *On the Recent Use of Local Binary Patterns for Face Authentication S?bastien Marcel, Yann Rodriguez and Guillaume Heusch // http://www.idiap.ch/~marcel/professional/publications/marcel-ijivp-*2007.*pdf*

12. Болл Р.М. Руководство по биометрии. – М.:Наука: 2011. – 460 с.

13. *Pentland, A.* & *Turk, M.* (1991). *Eigenfaces for Recognition. Journal of Cognitive Neuroscience* 3(1): 71-86.

14. *Saha, G.* & *Sandipan, C.* & *Suman, S.* (2004). *A New Silence Removal and Endpoint Detection Algorithm for Speech and Speaker Recognition Applications. Indian Institute of Technology, Khragpur*.

15. *Srinivasan. A.* (2012). *Speaker Identification and Verification using Vector Quantization and Mel Frequency Cepstral Coefficients. Research Journal of Applied Sciences, Engineering and Technology* 4(1), 33-40.

16. Визильтер Ю.В., Желтов С.Ю., Князь В.А. и др. Обработка и анализ цифровых изображений с примерами на *LabVIEW* и *IMAQ Vision*. – *М.*: ДМК Пресс, 2007. – 464 с.

17. Головко В.А. Нейронная сеть для иерархической классификации образов // Идентификация образов. – Минск:ИТК, 1999.-С.85-88.

18. Дуда Р.О., Харт П.Е. "Распознавание образов и анализ сцен." – М.: Мир, 1976.

19. Дьяконов В., Круглов В. *MATLAB*. Анализ, идентификация и моделирование систем: Специальный справочник. – СПб.: Питер, 2002.

20. Ковалёв В.А. Совмещение двумерных и трёхмерных изображений нежёстких объектов // Цифровая обработка изображений. – Минск:ИТК, 1999.-С.157-165.

21. Коваленко Е.Н., Сытник А.В. Методы выделения номерного знака на изображении // *V* Междунар. конф. "Интеллектуальный анализ информации ИАИ-2005". – 2005. – *С.* 167177.

22. Лосев С. Перспективы параллельных вычислений на *GPU* от *Nvidia* – *Hard'n'Soft,* №6 2009. *www.nvidia.eu/cuda/files/HardnSoft*_026_027_*trends*_ *Cuda.pdf*

23. Методы компьютерной обработки изображений / Под ред. В.А. Сойфера. – М.: Физматлит, 2001. – 784 с.

24. Бойченко С.В., Іванченко О.В. Положення про дипломні роботи (проекти) випускників Національного авіаційного університету. – К.: НАУ, 2017. – 63 с.

Додаток А

Лістинг коду основного програмного модуля

```
# import libraries
import cv2
import face_recognition

# Get a reference to webcam
video_capture = cv2.VideoCapture("/dev/video1")

# Initialize variables
face_locations = []

while True:

# Grab a single frame of video

ret, frame = video_capture.read()


# Convert the image from BGR color (which OpenCV uses) to RGB color (which face_recognition uses)

rgb_frame = frame[:, :, ::-1]


# Find all the faces in the current frame of video

face_locations = face_recognition.face_locations(rgb_frame)
```

```
# Display the results

for top, right, bottom, left in face_locations:

# Draw a box around the face

cv2.rectangle(frame, (left, top), (right, bottom), (0, 0, 255), 2)


# Display the resulting image

cv2.imshow('Video', frame)


# Hit 'q' on the keyboard to quit!

if cv2.waitKey(1) & 0xFF == ord('q'):

break

# Release handle to the webcam
video_capture.release()
cv2.destroyAllWindows()
# Initialize variables
face_locations = []
face_encodings = []
face_names = []
frame_number = 0
```

while True:

 # Grab a single frame of video

ret, frame = input_movie.read()

frame_number += 1

 # Quit when the input video file ends

if not ret:

break

 # Convert the image from BGR color (*which OpenCV uses*) *to RGB color* (*which face_recognition uses*)

rgb_frame = frame[:, :, ::-1]

 # Find all the faces and face encodings in the current frame of video

face_locations = face_recognition.face_locations(*rgb_frame, model*="*cnn*")

face_encodings = face_recognition.face_encodings(*rgb_frame, face_locations*)

face_names = []

for face_encoding in face_encodings:

 # See if the face is a match for the known face(*s*)

match = face_recognition.compare_faces(*known_faces, face_encoding, tolerance*=0.50)

name = None

if match[0]:

name = "Phani Srikant"

face_names.append(*name*)

 # Label the results

for (*top, right, bottom, left*), *name in zip*(*face_locations, face_names*):

if not name:

continue

 # Draw a box around the face

*cv*2.*rectangle*(*frame,* (*left, top*), (*right, bottom*), (0, 0, 255), 2)

 # Draw a label with a name below the face

```
cv2.rectangle(frame, (left, bottom – 25), (right, bottom), (0, 0, 255), cv2.FILLED)
    font = cv2.FONT_HERSHEY_DUPLEX

cv2.putText(frame, name, (left + 6, bottom – 6), font, 0.5, (255, 255, 255), 1)


# Write the resulting image to the output video file

print("Writing frame {} / {}".format(frame_number, length))

output_movie.write(frame)

# All done!
input_movie.release()
cv2.destroyAllWindows()
```