Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: **Методи та засоби біометричної ідентифікації користувачів в системі розумного будинку**

Виконав: студент(ка) 6 курсу, групи СІм-62
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

(підпис) Подвисоцький О. Є. (прізвище та ініціали)

Керівник (підпис) Стадник Н.Б. (прізвище та ініціали)

Нормоконтроль (підпис) Тиш Є.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« « грудня 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Подвисоцькому Олександру Євгеновичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи та засоби біометричної ідентифікації користувачів в системі розумного будинку*

Керівник роботи *Стадник Наталія Богданівна, кандидат технічних наук*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *01* « *грудня 2023* року № *4/7-1132*
2. Термін подання студентом завершеної роботи *28.12.2023 р.*
3. Вихідні дані до роботи *Алгоритми і засоби розпізнавання біометричних ознак людини*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1 Аналіз біометричних систем ідентифікації користувачів
2 Розробка архітектури системи РБ з біометричною ідентифікацією користувачів
3 Апробація методів біометричної ідентифікації особи в системі розумного будинку
4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Актуальність і мета дослідження.
2. Задачі дослідження, об'єкт і предмет, наукова новизна і практична цінність дослідження.
3. типова структура системи біометричної ідентифікації
4. Структурна схема розумного будинку з системою ідентифікації
5. Обґрунтування алгоритмів системи розпізнавання обличчя
6. Блок – схема роботи програми біометричної ідентифікації.
7. Експериментальне дослідження
8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Осухівська Г. М., зав. кафедри КС*		
Безпека в надзвичайних ситуаціях	*Стадник І. Я., професор кафедри ОХ*		

7. Дата видачі завдання *20.11.2023*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз сучасних біометричних систем ідентифікації користувачів*	*22.11.2023*	*Виконано*
2.	*Розробка архітектури системи розумного будинку з біометричною ідентифікацією користувачів*	*30.11.2023*	*Виконано*
3.	*Обґрунтування алгоритмів для системи ідентифікації користувачів*	*10.12.2023*	*Виконано*
4.	*Апробація методів біометричної ідентифікації*	*15.12.2023*	*Виконано*
5.	*Охорона праці та безпека в надзвичайних ситуаціях*	*18.12.2023*	*Виконано*
6.	*Оформлення пояснювальної записки і графічного матеріалу*	*19.12.2023*	*Виконано*
7.	*Попередній захист кваліфікаційної роботи магістра*	*20.12.2023*	*Виконано*
8.	*Захист кваліфікаційної роботи магістра*	*28.12.2023*	*Виконано*

Студент _____ *Подвисоцький Олександр Євгенович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник Наталія Богданівна*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби біометричної ідентифікації користувачів в системі розумного будинку // Кваліфікаційна робота магістра // Подвисоцький Олександр Євгенович // ТНТУ, комп'ютерна інженерія, група СІм-62 // Тернопіль, 2023 // с. – 77, рис. – 24, табл. – 2, бібліогр. – 26.

Ключові слова: розпізнавання облич, нейронні мережі, машинне навчання, ідентифікація особи, розумний будинок.

У кваліфікаційній роботі магістра досліджено методи і засоби біометричних методів ідентифікації особи в системі розумного будинку за біологічними особливостями обличчя.

Проведений аналіз біометричних ознак людини показав, що для реалізації в системі розумного будинку найбільш придатні біометричні показники: відбитки пальця, індивідуальні риси обличчя і голосу.

Формалізовано архітектуру системи керування розумним будинком з використанням системи біометричної ідентифікації

Здійснено підбір методів і алгоритмів обробки зображень з відеокамер для виявлення, розпізнавання і ідентифікації осіб по особливостях облич.

Розроблено програмне забезпечення, яке реалізовує описані методи і алгоритми для ідентифікації людини на базі біометричних ознак в системі розумного будинку

ABSTRACT

Methods and tools for biometric user identification in a smart home system // Master graduation thesis // Podvysotskyi Oleksandr Yevhenovych // TNTU, computer engineering, group CIm-61 // Ternopil, 2023 // p. – 77, fig. – 24, tab. – 2, bibliography. - 26.

Keywords: face recognition, neural networks, machine learning, person identification, smart home.

In the master's qualification work, the methods and means of biometric methods of identification of a person in the smart home system based on the biological features of the face were investigated.

The analysis of biometric features of a person showed that biometric indicators are most suitable for implementation in a smart home system: fingerprints, individual features of the face and voice.

The architecture of the smart home management system using the biometric identification system is formalized

The selection of methods and algorithms for image processing from video cameras for detection, recognition and identification of persons based on facial features was carried out.

Software has been developed that implements the described methods and algorithms for human identification based on biometric features in the smart home system.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ

SNoW (Sparse Network of Winnows) – алгоритм виявлення облич, який представляє собою двошарову мережу.

БНМ - багатошарова нейронна мережа.

НМ – нейронна мережа.

РБ – розумний будинок.

ЗНМ – згорткова нейронна мережа.

LBP (Local Binary Pattern) – локальні бінарні шаблони.

AAM (Active Appearance Models) – активні моделі зовнішнього вигляду.

ASM (Active Shape Models) – активні моделі форми

ВСТУП

Актуальність теми. Полягає у використанні біометричної ідентифікації, зокрема систем розпізнавання обличчя, за допомогою відеоаналітики для автоматизації керування системою розумний будинок. Враховуючи динамічний розвиток цих технологій та їх широкий спектр застосувань у відеоспостереженні, системах безпеки, торгівлі та транспорті, дослідження вважається актуальним.

Ринок відеоаналітики демонструє стабільний ріст з 2020 року. Це свідчить про активний розвиток та впровадження відеоаналітики в різних сферах. Однією з важливих задач відеоаналітики є розпізнавання облич у відеопотоках, що має практичне застосування в системах контролю доступу та ідентифікації особистості.

Дослідження біологічних методів ідентифікації людини є об'єктивно важливою проблемою, особливо з урахуванням зростання соціальних і комерційних застосувань біометричних технологій. Застосування розпізнавання облич у сферах кримінального розслідування, банківської сфери та інших галузях визначає практичну вигоду від використання цих технологій.

Незважаючи на прогрес у біометричних технологіях, завдання надійного розпізнавання обличчя залишається відкритим. Різноманітні методи використовуються для цього, такі як методи Віоли-Джонса, головних компонент, нейронні мережі тощо. Ці методи мають свої переваги та обмеження і вимагають подальших досліджень для оптимізації їхньої ефективності та стійкості до різних умов.

Основна увага в дослідженні спрямована на розробку методів, які були б ефективними за різних обставин, враховуючи різноманітні фактори, такі як освітлення, відстань, положення обличчя відносно об’єктива. Такий підхід спрямований на створення біометричних систем, які будуть надійними та ефективними в реальних умовах експлуатації розумного будинку.

Наукові дослідження та публікації в галузі біометричної ідентифікації користувачів в системі розумного будинку отримали велику увагу в останні роки. Ряд вчених вніс значний внесок у цю область, розробляючи та вдосконалюючи

методи та технології:

–Raghavendra Ramachandra: вивчає біометричні системи та їх застосування в розумних будинках. Його дослідження фокусуються на покращенні точності та швидкості біометричної ідентифікації.

–Arun Ross: спеціалізується на біометричних технологіях та має інтерес до їхнього використання в різних сферах, включаючи системи розумного будинку.

–Umberto Castellani: займається розробкою і вдосконаленням алгоритмів біометричної ідентифікації для використання в системах забезпечення розумного будинку.

–Mayank Vatsa: досліджує проблеми безпеки та ефективності в системах розумного будинку, використовуючи біометричні методи.

Ці вчені і їхні наукові групи досліджують різні аспекти, такі як розпізнавання обличчя, відбитків пальців, інші біометричні характеристики та їх використання для підвищення безпеки та зручності в системах розумного будинку. Вони активно публікують результати своїх досліджень у визнаних наукових журналах та конференціях, сприяючи розвитку цієї перспективної галузі.

Мета кваліфікаційної роботи полягає в розробці біометричних методів ідентифікації людини в системі розумного будинку.

Для того, щоб досягти мети, необхідно вирішити наступні задачі:

– провести аналіз сучасних методів біометричної ідентифікації;

– розглянути основні методи і алгоритми для системи ідентифікації по обличчю;

– розробити архітектуру системи керування розумним будинком з використанням біометричних заходів;

– здійснити програмну реалізацію запропонованої системи біометричної ідентифікації в системі розумного будинку;

– підтвердити шляхом експерименту ефективність реалізованої системи біометричної ідентифікації людини.

Об'єкт дослідження: система біометричної ідентифікації особи.

Предмет дослідження: алгоритм ідентифікації особи по біометричним даним

обличчя на базі машинного навчання.

Методи дослідження: методи системного аналізу та дослідження операцій; методи розпізнавання та класифікації образів, методи моделювання та теорії ймовірності.

Наукова новизна розроблено метод біометричної ідентифікації осіб в системі розумного будинку на основі алгоритмів розпізнавання облич з зображень відеокамер, що дає можливість автоматизувати налаштування параметрів розумного будинку відповідно до користувача.

Практичне значення результатів кваліфікаційної роботи результати дослідження можуть бути використані для подальшого розвитку та оптимізації систем розумного будинку з використанням біометричних методів ідентифікації.

Публікації. Результати дослідження апробовано на XI науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології», XII міжнародній науково-технічній конференція молодих учених та студентів «Актуальні задачі сучасних технологій», у вигляді тез конференцій.

1. Подвисоцький О., Стадник Н. Методи розпізнавання облич в системах ідентифікації користувачів розумного будинку. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С.98

2. Подвисоцький О., Стадник Н. Методи біометричної ідентифікації в розумному будинку. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 435.

Структура роботи. До складу кваліфікаційної роботи магістра входить розрахунково-пояснювальна записка та графічний матеріал. Розрахунково-пояснювальна записка містить вступ, 4 розділи, загальні висновки, список використаної літератури і додатки. Обсяг роботи: розрахунково-пояснювальної записки – 77 арк. формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

1.1. Процес і методи ідентифікації суб'єктів

Процес ідентифікації суб'єктів на даний момент дуже розвинений у світі і не є нововведенням. На даний момент можна виділити основні 3 групи, за якими можна ідентифікувати людину:

1) По фізичному предмету — будь-яка фізична річ, яка належить конкретній людині або відноситься до неї, як-от ключі, паспорт, смарт-картки або дані на носії, які доступні тільки цій людині.

2) За певним знанням - будь-яка інформація, яка зберігається в секреті і знання про яку є тільки у певної людини або групи осіб, наприклад пароль, секретна фраза або пін-код. Ці знання також можуть не представляти конфіденційну інформацію, яка може бути і не секретною, наприклад дівоче прізвище матері або улюблений колір.

3) За біометричними параметрами - це поведінкова чи фізіологічна характеристика людини. Це частини людського тіла чи дії, якими можна розрізняти людей друг від друга. Формально можна використовувати будь-яку особливість, яка є індивідуальною.

Ці три способи автентифікації можна використовувати як окремо, так і в сукупності, наприклад: введення номера телефону, який є загальнодоступним і введення пароля, який є секретною інформацією.

Ідентифікація, її можливо порівняти з біометричним «підписом». Тут використовується визначення того, кому належить той чи інший параметр, де йде порівняння з усіма записами про всіх людей у системі, наприклад: відбиток пальця, з вже наявною базою даних.

Верифікація порівнює отримані характеристики з вже раніше отриманими даними від цієї ж людини, щоб оцінити належність цих параметрів. Наприклад: на виробничих об'єктах, при надходженнях на роботу, відбитки людини заносяться в

базу, щоб коли людина приходила на роботу, їй потрібно було лише прикласти палець для перевірки її особи і надалі її надання прав. На відміну від ідентифікації, мається на увазі, що параметри людини вже є в системі, і вона однозначно може її визначити (відсоток відповідності є вкрай високим).

Один із затребуваних суб'єктів для ідентифікації є сама людина. Використання біометричних параметрів дуже складний процес, через складність їх отримання, через великі енерговитрати, а також є проблеми з тим, як їх порівнювати або знаходити відсоток схожості між параметрами.

Тому в основному можна бачити, як верифікація в основному відбувається за одним або двома параметрами.

Найпоширенішим і найпопулярнішим методом зараз є машинний зір [12]. Він застосовується досить широко для розпізнавання осіб та у системах відео спостережень. Хоч і багато вже є готових продуктів, напрацювань та досліджень, зараз досі ведуться нові дослідження та розробки в цій галузі [4, 5], багато існуючих систем мають ряд проблем з пов'язаних з [11, 13]:

–складність алгоритму: багато систем побудовано на базі складних алгоритмів, через чого з'являється необхідність в більше досконалих пристроях для обробки і аналізу даних.

–багатопотоковість: багато систем не вміють працювати коли необхідно знати кількох суб'єктів у кадрі або в потоці.

–стійкість: багато систем починають значно гірше працювати вже за мінімальних завад.

–точність: це залежить як від самого алгоритму, так і від кількості вхідних параметрів для аналізу суб'єкта.

З точки зору розпізнавання, практично всі методи можна представити у вигляді абстрактної системи R, що складається з трьох множин:

$$R = \langle A, S, P \rangle, \tag{1.1}$$

де A - набір виділених класів, S - перелік ознак, з допомогою яких можна віднести образ до того чи іншого класу з множини, P - набір правил за допомогою яких можна здійснити вибір відношення певного образу до конкретного класу.

Множини A і S складають інформаційну компоненту системи розпізнавання та тісно пов'язані. Від того, як вони описані [10, 14], може залежати той чи інший метод розпізнавання. Наприклад:

–Принцип порівняння з еталоном - клас описується одним або декількома еталонними образами.

–Принцип кластеризації – клас описується набором обмежень ознак.

–Принцип спільності властивостей - відповідає способу задання множин породжуючою процедурою, яка визначає в якості образів елементи цієї множини.

Ці принципи визначають підхід до організації системи розпізнавання і дозволяють використовувати різноманітні методи, залежно від конкретних вимог та умов застосування.

1.2. Біометричні характеристики людини

Перше, що необхідно зробити для побудови системи, це виділити всі характеристики об'єктів, що вивчаються, тобто їх біометричні характеристики. Біометричних ідентифікаторів існує велика кількість, але для порівняння будуть взяті тільки ті ідентифікатори, які оптимально використовувати в системі розумного будинку.

Якщо розглянути рис. 1.1 то можна побачити певну тенденцію розвитку систем біометричної ідентифікації людини.

Одна з перших широко поширених систем ідентифікації людини це сканери унікального папілярного рис. на пальцях людини. На даний момент поява мобільних, невеликих сканерів дозволяє застосовувати ці біометричні характеристики для ідентифікації особи людини навіть в мобільних пристроях.

Наступним видом біометричної ідентифікації є розпізнавання обличчя. Класичні системи використовують в аналізі плоскі зображення особи (2D портрети).

Двовимірний аналіз використовує певні точки та геометричні параметри, такі як відстані між центрами очей або між лінією очей та кінчиком носа.

Рис. 1.1. Розподіл використання біометричних ознак в сфері ідентифікації особи

Взагалі можна виділити два етапи або напрямки розвитку засобів біометричної ідентифікації осіб за обличчям. Перший напрямок аналізує плоскі двовимірні зображення особи. Двовимірний аналіз полягає в визначенні характерних точок та обчисленні геометричних параметрів, таких як відстані між центрами очей або між лінією очей та кінчиком носа. Двовимірний аналіз обмежений у здатності надавати багато біометричної інформації. Тому на даний час відбувається перехід до тривимірного аналізу геометрії лиця особи, що дозволяє значно розширити обсяг отримуваної інформації.

Рукописний почерк, а також клавіатурний почерк, як динамічна характеристика, пов'язана з особливостями поведінки людини. Тут аналізуються статистичні характеристики які отримують з пера або клавіатури.

Голосові характеристики також використовуються в системах розпізнавання голосу. Розпізнавання здійснюють на основі характеристик мови у вигляді коливань і розподілу частот

Серцевий ритм і характеристики манери ходьби людини не використовуються через недостатню унікальність біометричних параметрів, а також через проблематичність зняття показів.

Є й інші біологічні параметри які в тій чи іншій мірі можна використати в якості основи системи ідентифікації особи:

–діагностика підпису: у різних людей вона різна, де під час написання підпису враховується як сам рис., а й як його було нанесено [10];

–жести рук: в області машинного зору є одним із перспективних завдань, оскільки показує гарний відсоток відповідності, а також дозволяє отримувати унікальні дані, такі як будова кисті [8];

–райдужна оболонка: у багатьох можна побачити різний тон кольору очей, і навіть рис. оболонки [9];

–судини долоні: з'явилося щодо нещодавно в системах контролю та управління доступом (СКУД) [13];

–термографія особи: широко застосовується у методах діагностики захворювань та динамічного контролю у процесі лікування пацієнта [14].

Висвітлені позитивні властивості біометричних характеристик свідчать про їхню важливість та вигоду в контексті біометричних систем ідентифікації. іометричні системи дозволяють здійснювати ідентифікацію без прямого контакту з користувачем, що забезпечує зручність та відсутність неприємного втручання, використання біометричних характеристик гарантує високий рівень точності та надійності при визначенні особи, оскільки біометричні ознаки важко підробити чи скопіювати, система стає більш стійкою до шахрайства та несанкціонованого доступу. Процес ідентифікації на основі біометричних характеристик може бути швидким та ефективним, що дозволяє використовувати його в різних сферах.

1.3. Підбір і обґрунтування оптимальних біометричних ідентифікаторів

Розглянувши та оцінивши частину біометричних параметрів з параграфа 1.2, можна скласти формулу оцінки та оцінити всі вище описані біометричні параметри. Введемо кілька нових параметрів, за допомогою яких можна буде калібрувати результат під різні потреби:

– k_c - потреба в дешевизні. Чим більше, тим дешевше потрібно рішення.

– k_q - потреба в якості. Чим більше, тим точніше потрібно рішення.

– k_s - потреба у зручності. Що більше, то швидше має відбуватися ідентифікація суб'єкта.

Напишемо формулу (1.2) для визначення якості ознаки:

$$S = \frac{\frac{\text{загальн.+ унік.+ сталість + ефект.+ захищ.}}{5} \cdot 2^{\frac{k_q}{k_s}}}{\text{ціна+вимірюваність}+\frac{(\text{з}-\text{прийнятність})k_s}{2}} + \frac{\frac{\text{дом.+ мобіль.+ загаль.міс.}}{3} \cdot \frac{\text{зручн+експл.}}{2} \cdot \text{масовість} \cdot 2^{\frac{k_s}{k_q}}}{\frac{\text{ціна+вимірюваність}+(\text{з}-\text{прийнятність})k_c}{2}} \quad (1.2)$$

Для розгляду ідентифікаторів візьмемо наступні коефіцієнти:

$$k_c = 1, k_q = 1, k_s = 1,$$
$$k_c = 2, k_q = 1, k_s = 1,$$
$$k_c = 1, k_q = 2, k_s = 1,$$
$$k_c = 1, k_q = 1, k_s = 2,$$
$$k_c = 2, k_q = 2, k_s = 1,$$
$$k_c = 1, k_q = 2, k_s = 2,$$
$$k_c = 2, k_q = 1, k_s = 2\ .$$

А також знайдемо середнє значення по всім цим вхідним коефіцієнтам, які будемо використовувати далі. Підставивши усі значення отримуємо наступну таблицю (рис.1.2):

№	Біометричні параметри	1,1,1	2,1,1	1,2,1	1,1,2	2,2,1	1,2,2	2,1,2	Середнє
6	Відбитки пальців	18,13	12,09	12,27	33,07	8,18	18,13	22,04	17,70
1	Розпізнавання обличчя	13,04	5,22	9,88	22,72	3,95	13,04	9,09	10,99
2	Розпізнавання голосу	10,28	4,11	7,06	18,64	2,82	10,28	7,46	8,66
9	Термографія особи	9,12	3,65	7,44	15,36	2,98	9,12	6,14	7,69
21	Райдужна оболонка	8,47	4,23	6,93	14,23	3,47	8,47	7,12	7,56
22	Клавіатурний почерк	8,47	4,23	6,93	14,23	3,47	8,47	7,12	7,56
3	Жести рук	8,86	2,53	6,14	16,00	1,76	8,86	4,57	6,96
12	Судини долоні	7,60	3,80	6,20	12,80	3,10	7,60	6,40	6,79
8	Стиль почерку	7,76	3,10	6,52	12,88	2,61	7,76	5,15	6,54
11	Діагностика підпису	6,27	2,51	5,53	10,13	2,21	6,27	4,05	5,28
13	Колір шкіри	6,27	2,51	5,53	10,13	2,21	6,27	4,05	5,28
4	Швидкість кроків	6,71	1,92	5,93	10,86	1,69	6,71	3,10	5,28
10	Розмір кроку	5,70	2,85	6,15	8,10	3,08	5,70	4,05	5,09
5	Маса тіла	5,01	2,01	4,43	8,11	1,77	5,01	3,24	4,23
7	Зріст	2,45	1,23	3,03	3,10	1,51]	2,45	1,55	2,19
25	Колір волосся	2,63	0,88	3,52	3,07	1.17	2,63	1,02	2,13
18	Стать	2,35	0,59	2,83	3,05	0,71	2,35	0,76	1,80
19	Раса	1,94	0,56	3,03	1,83	0,87	1,94	0,52	1,53
20	Вік	1,87	0,62	2,73	1,93	0,91	1,87	0,64	1.51

Рис1.2. Таблиця ваг біометричних ідентифікаторів

Як видно з даної таблиці одні з кращих біометричних ідентифікаторів з допомогою яких можна розпізнати користувача системи розумного будинку є відбитки пальців, розпізнавання обличчя, голосу.

Поділимо біометричні ідентифікатори на групи:

1) Знаходження груп людей - ідентифікатори, за допомогою яких можна знаходити людину або певну групу людей у великій масі людей.

2) Ідентифікація людини (віддалено) - ідентифікатори, за допомогою яких можна ідентифікувати конкретну людину в малих групах людей, без прямої взаємодії. Наприклад, через камеру спостереження.

3) Ідентифікація людини (особисто) - ідентифікатори, за допомогою яких можна ідентифікувати конкретну людину, за допомогою прямої взаємодії на місці. Наприклад, через датчик відбитків пальців.

4) Ідентифікація людини (приватні) - ідентифікатори, за допомогою яких можна ідентифікувати конкретну людину, без прямої взаємодії з нею, але маючи вихідні дані про неї. Наприклад, отримавши пробу крові чи ДНК людини.

Опишемо біометричні ідентифікатори по наступною шкалою:

– низька - неможливо провести ідентифікацію біометричної ознаки;

– середня - біометричний ознака ідентифікується, але з найгіршими показаннями точності;

– висока - біометрична ознака добре ідентифікується на місці.

Застосуємо це до нашим біометричним ідентифікаторам в таблиці 1.1.

Таблиця 1.1

Групування біометричних методів по їх придатності для різних потреб

Біометрія	Груп людей	Ідентифікація (віддалено)	Ідентифікація (особисто)	Ідентифікація (приватні)
Вік	С	С	С	В
Діагностика підпису	Н	Н	С	В
Жести рук	С	С	В	В
Клавіатурний почерк	Н	С	С	В
Обличчя	С	В	В	В
Маса тіла	Н	Н	В	С
Відбитки пальців	Н	Н	В	С
Стать	Н	С	С	В
Райдужна оболонка	Н	Н	В	С
Розмір кроку	С	С	В	С
Раса	С	С	С	В
Розпізнавання голоси	Н	С	В	В
Зріст	С	С	В	С
Швидкість кроку	С	С	В	С
Судини долоні	Н	Н	В	С
Термографія особи	С	С	В	С
Колір волосся	С	С	В	В
Колір шкіри	С	С	С	В
Частини тіла	С	С	С	В

Для майбутньої системи будуть взяті біометричні ідентифікатори, щоб знайти конкретну людину з потоку в якійсь певній зоні, коли відомі усі люди допуск у яких є. Наступні біометричні ідентифікатори будуть взяті за основу в даній роботі:

– обличчя. Можна перевірити з використанням системи відеонагляду, яка зазвичай є частиною системи розумного будинку;

– відбитки пальців. Можна перевірити з допомогою пристроїв зчитування

відбитків пальців на багатьох пристроях (електричні замки, домофони, мобільні пристрої), які підключені до системи розумного будинку.

1.4. Характеристика класичних біометричних систем

Біометричні системи призначені для контролю доступу [3, 4, 5] до приватних приміщень та використовуються на різноманітних об'єктах. Проста БС виконує процес формування біометричного відбитку користувача за допомогою спеціалізованого обладнання, записує і обчислює його характеристики та параметри і порівнює його із збереженими параметрами і надає результат ідентифікації особи.

Типова структура біометричної системи (рис. 1.3.), яка використовується для ідентифікації користувачів складається з окремих модулів.

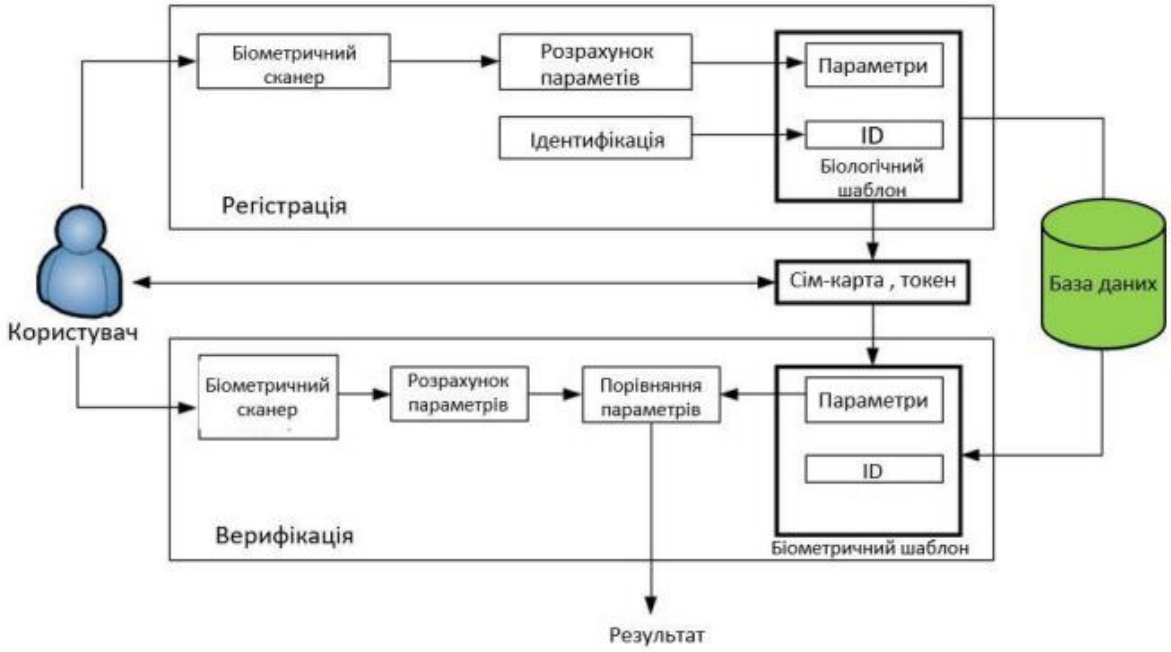

Рис. 1.3. Типова структура біометричної системи

Вона може бути описана наступним чином:

1. Реєстраційна підсистема:

– збір біометричних даних: Включає в себе процес зчитування біометричного образу користувача за допомогою біометричного пристрою введення,

такого як сканер відбитків пальців, сканер обличчя або інші біометричні сенсори;

– визначення ключових параметрів: Аналіз отриманих даних для виділення суттєвих характеристик користувача, таких як унікальні особливості відбитків пальців, геометрія обличчя тощо;

– створення біометричного шаблону: На основі визначених параметрів формується унікальний біометричний шаблон, який буде використовуватися для порівняння при подальших ідентифікаційних процесах.

2. Зберігання даних:

– ідентифікатор користувача: Кожному користувачу присвоюється унікальний ідентифікатор, який пов'язаний з його біометричним шаблоном;

– база даних: Біометричні шаблони та ідентифікатори зберігаються в базі даних для подальшого використання в процесі ідентифікації.

3. Ідентифікаційна підсистема:

– пред'явлення ідентифікатора та біометричних даних: Користувач пред'являє системі свій ідентифікатор та біометричні дані для вхідного контролю;

– порівняння параметрів: Біометричні дані порівнюються зі збереженими параметрами в базі даних для визначення ідентичності користувача;

– прийняття рішення: На основі порівняння приймається рішення про те, чи належать біометричні дані даного користувача чи ні.

4. Система відповіді:

– результат ідентифікації: Видається результат в формі «Так» або «Ні» щодо ідентифікації користувача;

– додаткові дії: Залежно від результату, система може виконувати додаткові дії, такі як відкриття дверей або відмова в доступі.

Ця структура дозволяє біометричній системі ефективно та безпечно ідентифікувати користувачів на основі їх унікальних біометричних характеристик

1.5. Нейромережеві засоби в біометричних системах ідентифікації

Нейромережеві перетворювачі біометричного коду використовують навчену нейронну мережу для формування значення ключа. На етапі біометричної реєстрації користувача створюється ключ із значенням key і на цьому ключі здійснюється навчання нейронної мережі без участі людини (Вчителя). На рис. 1.4 показано загальна схема навчання.

Крім ключа для навчання нейронної мережі потрібні вибірки (Приклади) двох класів образів - «Свій» і «Чужий», представлені в вигляді векторів біометричних параметрів VCв і VЧж відповідно. Передбачається навчання на безперервних і дискретних біометричних параметри.

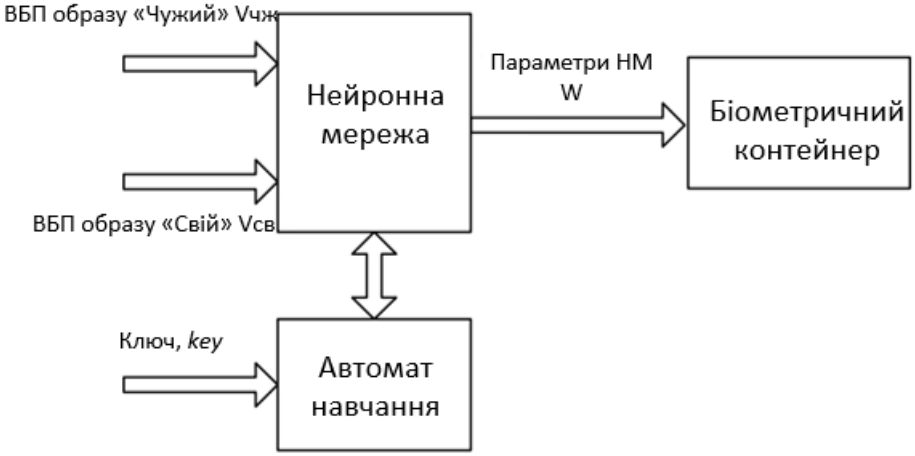

Рис.1.4. Загальна схема процедури автоматичного навчання нейромережевого перетворювача біометричного-коду

Крім ключа потрібно вектор для біометричних параметрів (ВБП) «Свій» і «Чужий». Ці набори використовуються для навчання нейронної мережі.

Формально нейронна мережа описується матрицею вагових коефіцієнтів W або таблицями зв'язків нейронів і таблицями вагових коефіцієнтів, які містяться в біометричному контейнерв для наступного відновлення ключа. Процес навчання ІНС необхідний обчислення W так, щоб при вплив на її (подання на її входи) прикладами образу

«Свій» на виходах ІНС формувалося точне значення ключа *key* . Загальна схема нейромережевого перетворення біометрія-код представлена на рис. 1.7. При вплив на ІНС прикладами образу «Чужий» на виходах ІНС повинні формуватися випадкові вихідні коди.

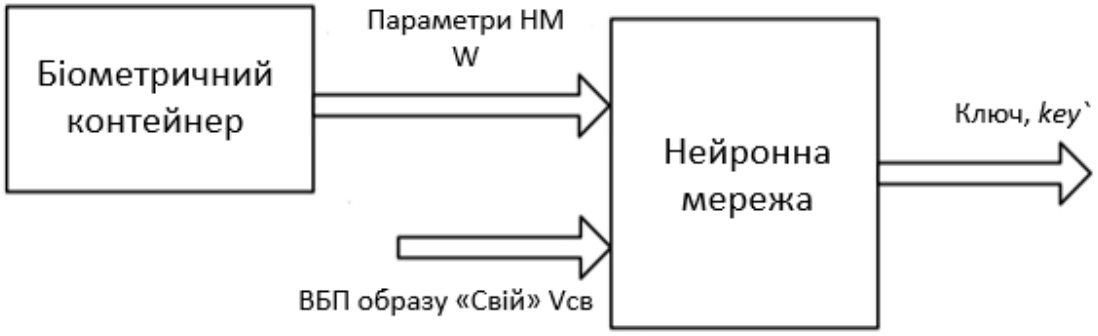

Рис. 1.7. Загальна схема нейромережевого перетворення біометричного коду

Перевагою нейромережевих перетворювачів біометричного коду вважаються хешуючі властивості нейронної мережі, які можуть бути значнопосилені механізмом збільшення проміжних кодів біометричних перетворень, заснованомих на додаванні за модулем два даних з ще не використаних нейронів із фрагментами вже отриманого попередніми нейронами вихідного коду доступу або криптографічного ключа.

Висновок до 1 розділу.

Отже в рамках даного розділу була проаналізована предметна область біометричної ідентифікації людини.

Були визначені і досліджені основні біологічні ознаки з допомогою яких ідентифікують людей.

Зважаючи на велику кількість ознак були визначені найбільш оптимальні для використання в системі ідентифікації розумного будинку.

РОЗДІЛ 2
РОЗРОБКА АРХІТЕКТУРИ СИСТЕМИ РОЗУМНОГО БУДИНКУ З БІОМЕТРИЧНОЮ ІДЕНТИФІКАЦІЄЮ КОРИСТУВАЧІВ

У цьому розділі розглядаються питання щодо вибору технологій, що застосовуються для побудови системи домашньої автоматизації, проводиться опис розробленої архітектури, здійснюється вибір пристроїв і алгоритмів ідентифікації користувачів для системи управління «розумним будинком»

2.1. Формалізація архітектури системи керування розумним будинком з використанням біометричних засобів

Як вже згадувалось в попередньому розділі в даній роботі буде розглядатись дві системи ідентифікації користувачів в системі розумного будинку. На рис. 2.1 наведена архітектура системи розумного будинку з біометричною ідентифікацією за відбитком пальця і розпізнаванням обличчя користувача.

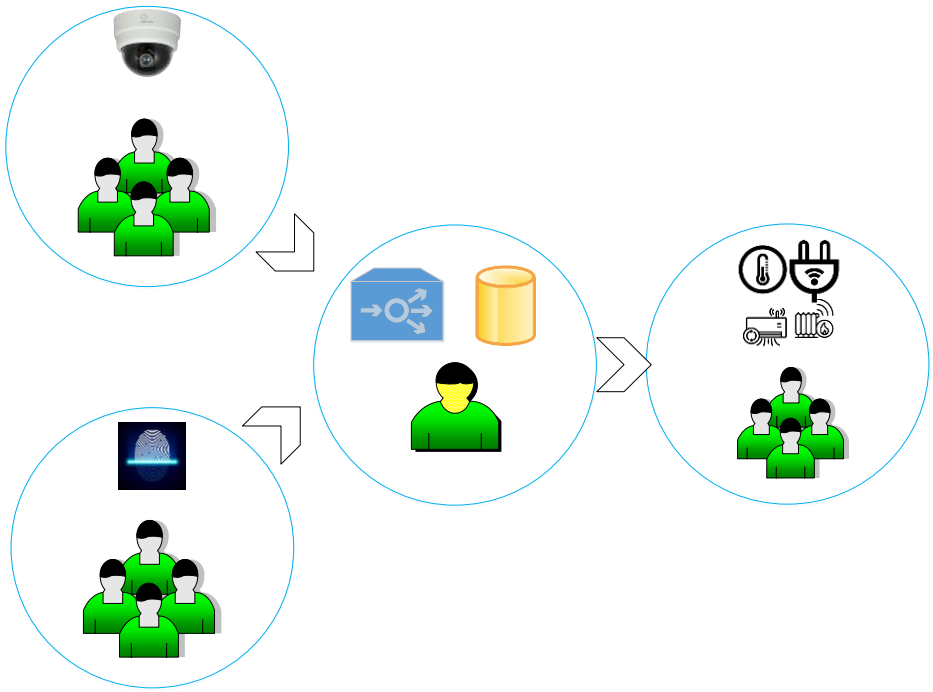

Рис.2.1. Загальна структура розумного будинку з системою біометричної ідентифікації користувачів

Передбачимо, що в системі розумного будинку вже створені профілі користувачів (параметри налаштування обладнання і доступу).

Користувачі можуть ідентифікувати себе з використанням сканера відбитків, який може бути вмонтований в електронні замки, домофон або в мобільні пристрої з системою керування параметрами розумного будинку. Відповідно система розпізнає відбиток пальця, здійснить перевірку і звірку в біометричній базі користувачів наявності користувача і дасть рішення «Свій» чи «Чужий».

Таким чином користувачу буде надано чи заборонено доступ до приміщень чи налаштувань системи розумного будинку.

Інший варіант ідентифікації полягає у розпізнаванні користувача з використанням системи відеонагляду розумного будинку. Тобто на основі розпізнавання атрибутів лиця з відеоряду.

Цей процес дещо складніший, але він дозволить ідентифікувати користувача і, наприклад, здійснити налаштування параметрів мікроклімату приміщення в залежності хто в ньому знаходиться. Систему прийняття рішень на основі динамічного користувацького профілю розглянуто в роботі [18].

Після вибору основних технологій біометричної ідентифікації, необхідно визначитися з архітектурою апаратних засобів розроблюваної системи управління елементами «розумного будинку».

Для побудови системи управління компонентами «розумного будинку» існують два основних принципи:

1) Децентралізований принцип (рис.2.2.) управління «розумним будинком» включає в себе розподіл функцій управління між різними пристроями та системами в будинку, щоб забезпечити ефективне та гнучке управління різними аспектами життя в будинку без необхідності централізованого контролю.

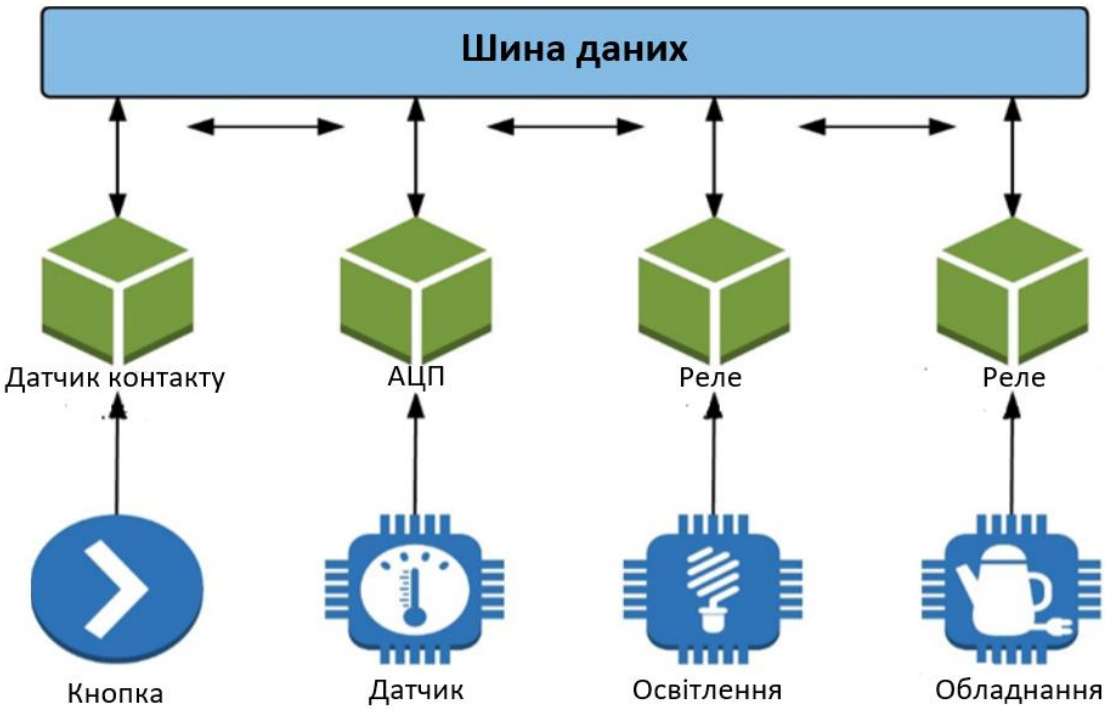

Рис. 2.2. Децентралізований принцип управління «розумним будинком»

Основні принципи цього підходу включають:

–Розподілене виконання завдань: Різні пристрої (освітлення, терморегуляція, безпека і т. д.) можуть мати вбудовані «розумні» функції, які дозволяють їм автономно приймати рішення на основі зібраних даних;

–Мережева взаємодія: Простежується тенденція до створення великої мережі зв'язку між різними пристроями в будинку. Це може включати протоколи зв'язку, такі як Zigbee, Z-Wave або Wi-Fi, щоб забезпечити ефективний обмін інформацією;

–Локальне управління: Важливим аспектом децентралізованого управління є можливість виконувати більшість функцій локально на самому пристрої без необхідності постійного звертання до централізованої системи;

–Система «розумного будинку» як платформа: Розумний будинок може виступати як платформа, яка дозволяє різним пристроям та додаткам взаємодіяти між собою, обмінюючи інформацією та командами через відкриті інтерфейси.

–Автономія: Принцип децентралізації також передбачає можливість пристроїв функціонувати автономно, навіть у випадку відсутності зв'язку з центральною системою або Інтернетом;

–Захист від кіберзагроз: Децентралізовані системи можуть мати покращені заходи безпеки, оскільки порушення безпеки на одному пристрої не обов'язково впливає на всю систему.

Застосування децентралізованих принципів управління розумним будинком сприяє підвищенню його гнучкості, ефективності та надійності. При цьому підході всі компоненти системи функціонують автономно і відсутній центральний контролер, що відповідав би за збір інформації, відправлення команд та прийняття рішень.

З урахуванням цієї структури і враховуючи обмежені обчислювальні ресурси окремих компонентів, важко реалізувати високоінтелектуальні алгоритми управління. Більшість сценаріїв використовують прості схеми, які можна важко назвати «розумними».

Переваги децентралізованих систем включають високу надійність, оскільки відмова одного або кількох модулів майже не впливає на загальну функціональність системи. Додатково, ці системи легко розширюються, адже додавання нових модулів на існуючу шину досить просте завдяки підтримці відповідного протоколу передачі даних.

Серед недоліків можна виділити високі витрати на децентралізовані системи порівняно з централізованими аналогами, а також обмежену швидкість роботи через розподіл обробки даних між різними модулями. Технічні труднощі та збільшення розміру системи також вважаються недоліками через використання модулів з власними контролерами обробки даних.

2) Централізований і розподілений (рис.2.3.) принципи управління «розумним будинком» представляють альтернативні підходи до організації системи. Розглянемо обидва принципи:

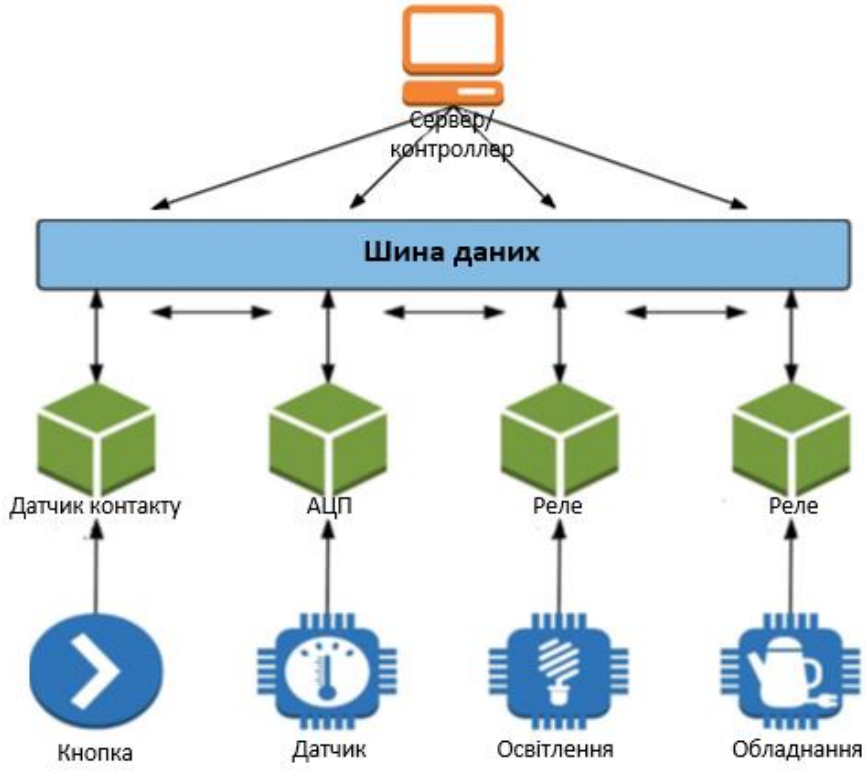

Рис.2.3. Централізований принцип управління «розумним будинком»

Централізований принцип управління: В централізованій системі «розумного будинку» всі елементи та пристрої пов'язані з центральним контролером. Цей контролер відповідає за збір, обробку і аналіз інформації, а також за видачу команд для керування різними аспектами будинку, такими як освітлення, температурне регулювання, безпека та інші.

Переваги централізованої системи:

–централізований контроль: Забезпечує централізований і високий рівень керування всіма аспектами будинку;

–швидкість прийняття рішень: Може дозволяти швидше прийняття рішень, оскільки вся обробка відбувається в одному центрі.

Недоліки централізованої системи:

–залежність від центрального вузла: Вихід з ладу центрального контролера може призвести до втрати контролю над всією системою.

–складніше розширення: Додавання нових елементів може виявитися складнішим, оскільки вони повинні бути інтегровані в централізовану інфраструктуру.

Розподілений принцип управління: У розподіленій системі «розумного будинку» кожен пристрій або елемент має власний вбудований інтелект та можливість приймати рішення автономно. Взаємодія між пристроями може відбуватися через локальну мережу.

Переваги розподіленої системи:

–незалежність пристроїв: Додавання нових пристроїв може бути простіше, незалежність пристроїв: Відсутність центрального контролера дозволяє пристроям працювати незалежно один від одного.

–легша розширюваність оскільки вони можуть працювати як самостійні вузли.

Недоліки розподіленої системи:

–складніше управління: В умовах розподіленої системи складніше забезпечити централізований та координований контроль над усіма пристроями.

–потреба в ефективній комунікації: Ефективна взаємодія між пристроями вимагає добре організованої мережної структури.

Обираючи між централізованим і розподіленим принципами, розробники «розумних будинків» враховують конкретні потреби та вимоги користувачів, а також визначаються завданнями, які передбачаються для системи.

Аналізуючи переваги та недоліки обох підходів до побудови системи «розумного будинку», приходжу до висновку, що в даному контексті централізований підхід є більш виправданим. Це особливо актуально, враховуючи конкретні вимоги до біометричної ідентифікації у системі «розумний будинок».

Централізований підхід дозволяє створити ефективний центр управління, який контролює всі аспекти системи. Це стає важливим у випадках, коли використовується біометрична ідентифікація, де важлива точність та безпека. Основні переваги централізованої системи включають забезпечення єдиної точки

контролю, швидше прийняття рішень та можливість ефективної інтеграції біометричних технологій.

Незважаючи на певні обмеження, такі як залежність від центрального вузла, цей підхід виглядає найбільш придатним для використання в рамках даної роботи, де біометрична ідентифікація визначає високі стандарти безпеки та надійності.

2.2. Вибір алгоритмів для системи ідентифікації по обличчю

Перед тим, як почати реалізовувати систему розпізнавання осіб потрібно вибрати алгоритми які лежатимуть у її основі. Вивчивши те, як влаштовані алгоритми, проаналізувавши їх позитивні і негативні якості, було прийнято рішення використати:

–гістограма напрямлених градієнтів (HOG) для виявлення особи;

–ансамбль дерев регресії (випадковий ліс) для побудови ключових точок;

–згорткова нейронна мережа (CNN) для обчислення ключових ознак;

–лінійний метод опорних векторів (SVM) для класифікації.

Розглянемо обґрунтування обраних алгоритмів і принцип їх роботи.

Для першого етапу порівняємо HOG з іншими методами локалізації,такими як вейвлети Хаара (що використовуються у методі Віоли-Джонса) таконтексти форми представлені в оригінальній роботі [14], де автори проводили тестування свого алгоритму на двох наборах даних з зображеннями людей, а саме MIT та IRNA [3].

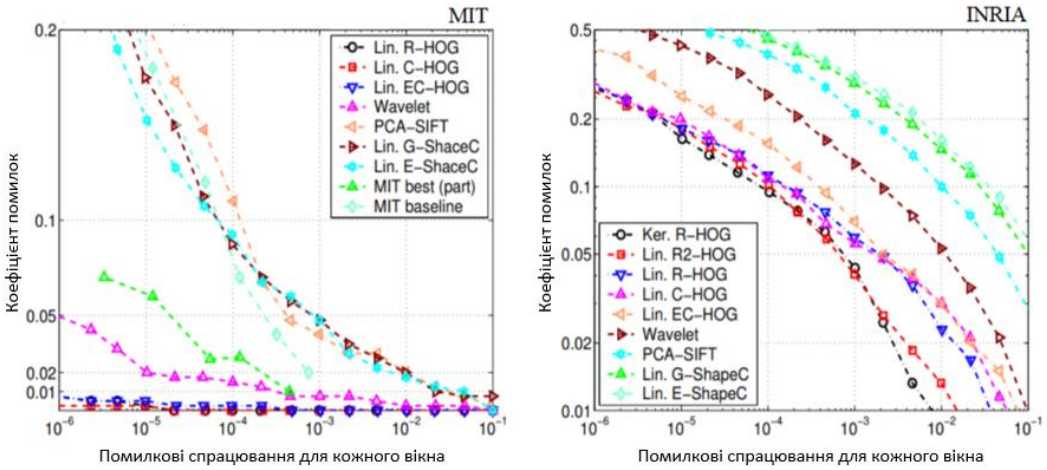

Рис. 2.4. Графік порівняльного аналізу

Таблиця 2.1

Порівняльний аналіз методів локалізації зображень

Дескриптор	Набір даних	Частка пропущених зображень	Частка помилок першого роду
HOG	MIT	≈0	0,0001
HOG	INRIA	0.1	0,0001
Вейвлети Хаара	MIT	0.01	0,0001
Вейвлети Хаара	INRIA	0.3	0,0001
PCA-SIFT, контексти форми	MIT	0.1	0,0001
PCA-SIFT, контексти форми	INRIA	0.5	0,00001

Також проводилися експерименти з використанням алгоритму HOG, як заміни згорткової нейронної мережі. Статистика всіх даних представлена рис. 2.5

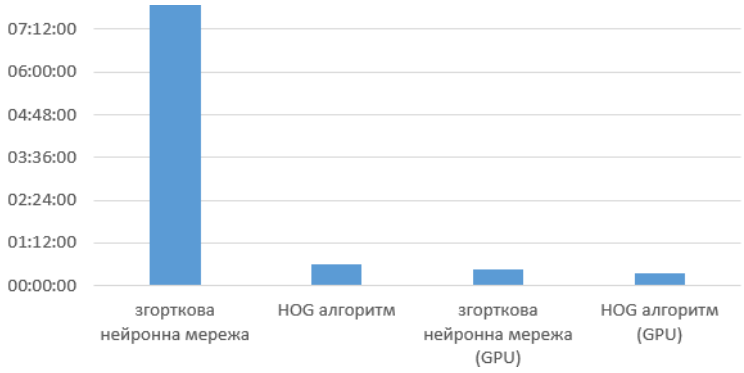

Рис. 2.5. Час роботи алгоритмів

Як видно, згорткові нейронні мережі є не самим оптимальним алгоритмом машинного навчання і використання HOG алгоритму для пошуку об'єктів набагато ефективніше справляється із завданням локалізації об'єктів. Але якщо використовувати потужності графічного процесора, то ситуація змінюється, і згорткові нейронні мережі практично зрівнюються по ефективності з HOG, це є наслідком використання однорідних математичних дій, і власне ефективність їх розпаралелювання.

2.2.1. Алгоритм HOG для виявлення осіб

«Вперше гістограма направлених градієнтів була представлена в роботі Навніт Далалом та Біллом Триггсом у червні 2005 р. Вони застосовували цей метод для розпізнавання пішоходів на статичних зображення. У В даний час цей метод широко використовується не тільки для знаходження пішоходів, але і розпізнавання осіб, автомобілів і інших об'єктів на відеопослідовності.» [13]

Алгоритм складається з векторного простору, яке обчислює подібність з використанням евклідових або косинусних відстаней, що добре підходить для методів машинного навчання. У його основі лежить припущення, що вигляд розподілу градієнтів інтенсивності зображення дозволяє достатньо точно визначити наявність і форму присутніх на ньому об'єктів [16].

Перший крок полягає у алгоритмах пошуку особливих точок, використовують нормалізацію кольору та гамма-корекцію, проте Далал і Тріггс з'ясували, що їх застосування принесе той самий результат, що й нормалізація.

Тому перший крок в алгоритмі HOG полягає в розрахунку значень градієнтів. Для цього використовуються застосуванні одновимірних похідних масок як в вертикальному, так і в горизонтальному напрямках. Розміри використовуваних тут масок - 1X3 та 3X1 (рис. 2.6).

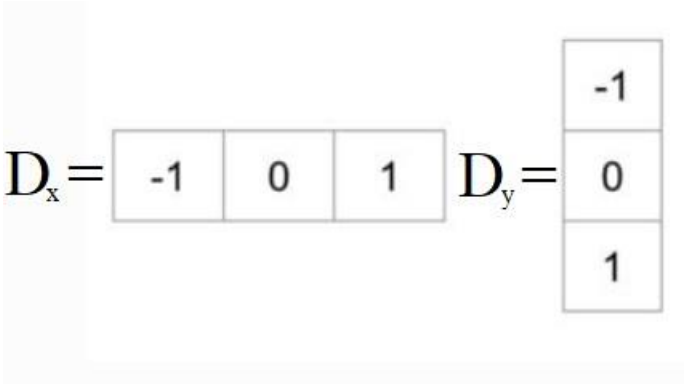

Рис. 2.6. Використовувані маски

Для обчислення градієнта в точці використовуються наступні формули (2.1-2.4):

$$G_x(x,y) = H(x+1,y) - H(x-1,y), \quad (2.1)$$

$$G_y(x,y) = H(x,y+1) - H(x,y-1), \quad (2.2)$$

$$G = \sqrt{G_x(x,y)^2 + G_x(x,y)^2}, \quad (2.3)$$

$$\theta(x,y) = \tan^{-1}\left(\frac{G_y(x,y)}{G_x(x,y)}\right), \quad (2.4)$$

де:G_x - горизонтальний градієнт крапки x, y; G_y – вертикальний градієнт крапки x, y; H - Значення пікселя x, y ;G - розмір градієнта x, y ; θ - напрямок градієнта x, y .

Результати обробки зображення алгоритмом з застосуванням різних масок можна спостерігати на рис. 2.7 (а-г) .

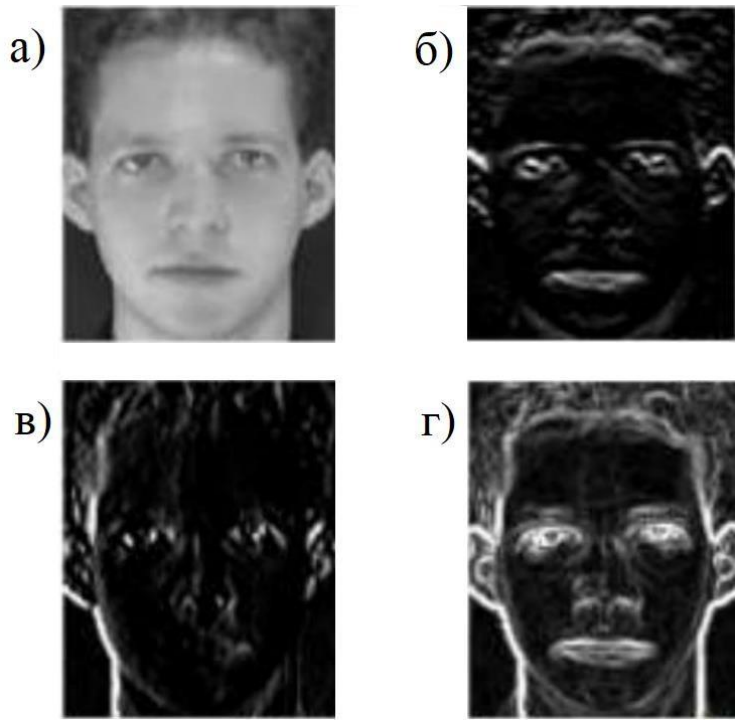

Рис.2.7. Обробка зображення алгоритмом з застосуванням різних масок

а - Зображення до застосування фільтрів;

б – результат застосування горизонтальної маски; в – результат застосування вертикальної маски; г – результат застосування вертикальної та горизонтальної маски одночасно.

На наступному етапі відбувається групування напрямків. Кожен піксель, ґрунтуючись на значенні і напрямку градієнта, передає своє значення в один з каналів (інтервалів) гістограми. Сама гістограма представляє собою вектор (або масив) чисел, в якому інтервали відповідають кутку градієнт. Таким чином, якщо величина градієнта дорівнює 5, а кут 20 градусів, тоді його значення буде записано в канал, відповідальний за цей кут. При обчисленні «знакового» градієнта – канали рівномірно розподілені від 0 до 360 градусів, в «беззнакове» вони розподіляються від 0 до 180 градусів. Значення пікселя во час голосування може бути задано коренем або квадратом градієнта або його абсолютним або урізаним значенням [6]. У час дослідження ефективності алгоритму було встановлено, що обчислення «беззнакового» градієнта та використання 9 каналів гістограми показує набагато більше високі результати під час розпізнавання людей.

На рис. 2.8(а) показано операцію угруповання напрямків. Зразок зображення особи розбитий на комірки. Рис. 2.8(б) представляє собою відповідні гістограми клітин.

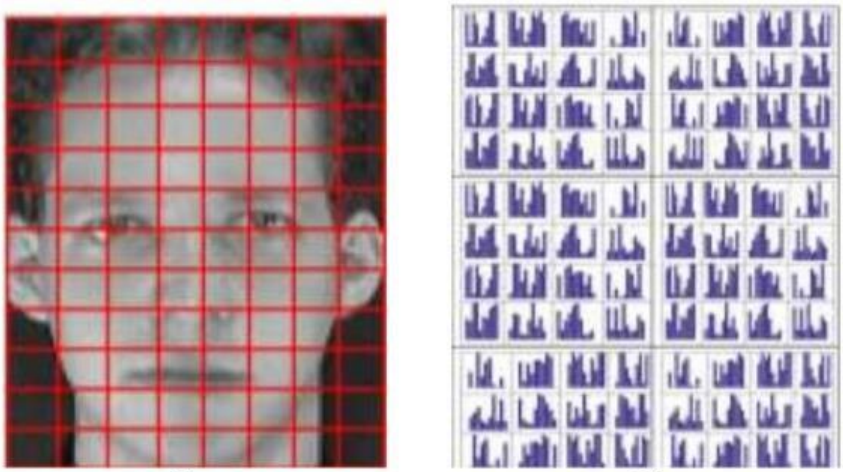

Рис. 2.8. Групування напрямів

Далі слід провести локальне нормування градієнтів для врахування змін контрасту та освітлення. Для цього потрібно згрупувати осередки в більш великі і просторово-пов'язані блоки. У цьому випадку дескриптор гістограми орієнтованих градієнтів є вектором компонент гістограм осередків, нормованих із усіх областей блоку. Ці блоки зазвичай перекриваються, що означає, що кожен осередок вносить свій вклад у остаточні дескриптори як мінімум більше одного рази.

Існує два типи геометрії блоків: прямокутні (R-HOG) і кругові (C-HOG) блоки гістограми направлених градієнтів.

Блоки R- HOG являють собою прямокутні або квадратні сітки, які характеризуються трьома параметрами: комірки на кожен блок, пікселі на кожен блок і канали на кожну гістограму.

У експерименті по виявленню людської особи найбільш сприятливими параметрами виявились чотири комірки 8X8 пікселів (16X16 пікселів у кожному блоці) з 9 каналами гістограми.

Наступним кроком потрібно здійснити нормалізація блоків. Коефіцієнт нормалізації можна отримати одним з наступних способів [13]:

$$L2-\text{норма}: f = \frac{v}{\sqrt{\|v\|_2^2+e^2}}, \tag{2.5}$$

$$L2-hys: f = \frac{v}{\sqrt{\|v\|_2^2+e^2}}\ if\ v > 0{,}2: v = 0{,}2\ , \tag{2.6}$$

$$L1-\text{норма}: f = \frac{v}{\sqrt{\|v\|_1+e}}, \tag{2.7}$$

$$1-\text{квадрат}: f = \frac{v}{\sqrt{\|v\|_1+e}}, \tag{2.8}$$

де v- ненормований вектор, містить усі гістограми в даному блоці, $\|v\|_k$ - k -норма цього вектора для k = 1,2, e - деяка мала константа.

У результатах дослідження Далал і Тріггс виявили, що схема L2- норма, L2-hys та L1-квадрат (2.5, 2.6, 2.8) мають приблизно рівну ефективність, а L1-норма (2.7) забезпечує менше надійну роботу. Але в підсумку усі методи показали значне покращення по порівнянні з ненормалізованими даними.

2.2.2. Класифікація даних методом опорних векторів (SVM)

Метод опорних векторів використовується для рішення завдань класифікації і регресії. Він представляє кожен об'єкт даних як вектор в просторі, кожен з яких належить одному з двох класів. Його мета - побудувати гіперплощину, яка розділяє ці два класу. Однак в результаті може бути побудовано безліч площин, тому потрібно вибрати таку, відстань до якої від прилеглої крапки кожного класу буде максимальним. Така розділяюча гіперплощина називається оптимальною [4].

Дана навчальна вибірка D , а набір даних складається з n об'єктів:

$$D = (x_1, y_1), \cdots, (x_n, y_n), \tag{2.9}$$

де y приймає значення 1 або −1 залежно від того, до якого класу відноситься точка x. Кожен x_i це p -мірний дійсний вектор, нормалізований значеннями [0,1] або [-1,1].

Ненормалізована точка з найбільшим відхиленням може суттєво вплинути на роботу класифікатора, тому необхідно провести їх нормування. Це можна розглядати як вибірку із заздалегідь заданим класом кожного елемента, до якого він відноситься. У результаті класифікатор повинен навчиться самостійно правильно розподіляти елементи за класами.

Для цього потрібно побудувати роздільну гіперплощину, що має наступний вид:

$$w \cdot x - b = 0\,, \tag{2.10}$$

де вектор w – перпендикуляр до розділюваної площини, b – допоміжний параметр. Параметр $\frac{b}{\|w\|}$ дорівнює по модулю відстані гіперплощини від початку координат. У випадку, коли $b = 0$ – гіперплощина проходить крізь початок координат, що обмежує рішення.

У випадку, коли дані є лінійно роздільними потрібно побудувати дві гіперплощини, які поділять точки на два класи. Далі слід максимізувати відстань між цими площинами і знайти оптимальну розділюючу гіперплощину, яка буде розташовуватися безпосередньо на підлога шляхи між ними. Розділюючі гіперплощини можуть бути описані рівняннями (2.11-2.12):

$$w \cdot x - b = 1\,, \tag{2.11}$$

$$w \cdot x - b = -1. \tag{2.12}$$

Таким чином, всі елементи на цій межі або вище належать класу 1 (2.11), а всі елементи на межі або нижче, належать до класу 2 (2.12).

Геометрична відстань між цими площинами дорівнює $\frac{2}{\|w\|}$, для того щоб максимізувати відстань, потрібно мінімізувати $\|w\|$. Щоб виключити влучання точок на поля, додається обмеження (2.13).

Для кожного i

$$\begin{cases} w \cdot x_i - b \geq 1, c_i = 1 \\ w \cdot x_i - b \leq -1, c_i = -1 \end{cases}. \quad (2.13)$$

Ці обмеження означають, що кожна точка даних має лежати на правильній стороні поля.

Це можна записати в вигляді (2.14):

$$c_i(w \times x_i - b) \geq 1, 1 \leq i \leq n\,. \quad (2.14)$$

Якщо поставлені вище умови (2.14) виконуються - завдання побудови оптимальної розділяючої зводиться до мінімізації $||w||$ і має вид (2.15):

$$\begin{cases} \|w\|^2 \to min \\ c_i(w \times x_i - b) \geq 1, 1 \leq i \leq n \end{cases}. \quad (2.15)$$

За теоремою Куна - Таккера дане задача еквівалентна подвійній задачі пошуку нижньої точки функції Лагранжа (2.16)

$$\begin{cases} L(w, b; \lambda) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{n} \lambda_i (c_i((w \cdot x_i) - b) - 1) \longrightarrow \min_{w,b}\max_{\lambda}, \\ \xi_i \geq 0, 1 \leq i \leq n \end{cases} \quad (2.16)$$

де $\lambda = (\lambda_1, \cdots, \lambda_n)$ – вектор двійкових змінних.

Далі слід звести цю задачу до еквівалентної задачі квадратичного програмування, що містить тільки двійкові змінні (2.17):

$$\begin{cases} -L(\lambda) = -\sum_{i=1}^{n} \lambda_i + \frac{1}{2}\sum_{i=1}^{n}\sum_{i=1}^{n} \lambda_i \lambda_j c_i c_j (x_i \cdot x_j) \longrightarrow \min_{\lambda}, \\ \lambda_i \geq 0, 1 \leq i \leq n, \\ \sum_{i=1}^{n} \lambda_i c_i = 0 \end{cases} \quad (2.17)$$

Припустимо що задачу вирішено. У такому випадку можна знайти w і b по наступним формулам (2.18), (2.19):

$$w = \sum_{i=1}^{n} \lambda_i c_i x_i, \tag{2.18}$$

$$b = w \cdot x - c_i, \lambda > 0. \tag{2.19}$$

У результаті алгоритм класифікації може бути записаний у вигляді (2.20):

$$a(x) = sign(\sum_{i=1}^{n} \lambda_i c_i x_i \cdot x - b) \tag{2.20}$$

При цьому підсумовування йде не по всій вибірці, а лише по опорним векторам, для яких $\lambda_i \neq 0$.

У випадку лінійно нероздільних даних, алгоритм може допускати помилки в процесі навчання. Для цього вводяться додаткові змінні $\xi_i \geq 0$, які характеризують величину помилки на об'єктах $x_i \geq 0, 1 \leq i \leq n$. Виходячи з виразу (2.16), обмеження нерівності пом'якшуються і в мінімізованому функціоналі додається «штраф» за сумарну помилку (2.21):

$$\begin{cases} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \xi_i \longrightarrow \min_{w,b,\xi_i}, \\ c_i(w \cdot x_i - b) \geq 1 - \xi_i, 1 \leq i \leq n, \\ \xi_i \geq 0, 1 \leq i \leq n \end{cases} \tag{2.21}$$

Тут коефіцієнт C є параметром, який регулює відношення між максимізацією ширини розділяючої смуги та мінімізацією сумарної помилки.

Згідно з теоремою Куна-Таккера, задачу зводять до пошуку нижньої точки функції Лагранжа (2.22):

$$\begin{cases} L(w,b,\xi;\lambda,\eta) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{n}\lambda_i(c_i((w\ \cdot\ x_i)\ -\ b) - 1) - \\ -\sum_{i=1}^{n}\xi_i(\lambda_i + \eta_i - C) \longrightarrow \min_{w,b,\xi}\max_{\lambda,\eta}\ \xi_i, \lambda_i, \eta_i \geq 0, 1 \leq i \leq n, \\ \begin{cases} \lambda_i = 0, \\ c_i(w\ \cdot\ x_i - \ b) = 1 - \xi_i, \end{cases} 1 \leq i \leq n, \\ \begin{cases} \xi_i = 0, \\ \eta_i = 0 \end{cases}, 1 \leq i \leq n. \end{cases} \tag{2.22}$$

За аналогією зведемо цю задачу до еквівалентної (2.23):

$$\begin{cases} -L(\lambda) = -\sum_{i=1}^{n}\lambda_i + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\lambda_i\lambda_j c_i c_j (x_i \cdot x_j) \longrightarrow \min_{\lambda}, \\ 0 \leq \lambda_i \leq C, 1 \leq i \leq n, \\ \sum_{i=1}^{n}\lambda_i c_i = 0 \end{cases} \tag{2.23}$$

Використовуючи метод опорних векторів, вирішується саме задача з формули (2.21), а не (2.17), оскільки гарантувати лінійну роздільність точок на два класи в загальному випадку неможливо. Цей варіант алгоритму відомий як алгоритм з м'яким зазором (soft-margin SVM), на відміну від лінійно роздільного випадку, який називається жорстким зазором (hard-margin SVM).

Для алгоритму класифікації зберігається формула (2.20), але з тою відмінністю, що тепер ненульові значення λ_i відповідають не тільки опорним об'єктам, але і об'єктам-шумам. У такому випадку виникає недолік у вигляді побудованого на їх рішенні правила.

Константу C зазвичай обирають за критерієм ковзного контролю. Цей спосіб є трудомістким, оскільки задачу доводиться вирішувати повторно для кожного значення C.

Є ситуації, коли лише об'єкти-викиди заважають правильній класифікації лінійної вибірки. Для вирішення цієї проблеми використовується фільтрація викидів. Спочатку задача розв'язується при певному значенні C і з вибірки вилучається невелика частина об'єктів з найбільшими значеннями помилки ξ_i. Після цього задача розв'язується знову на відфільтрованій вибірці. Можливо, знадобиться кілька ітерацій, поки інші об'єкти не стануть лінійно роздільними.

2.2.3. Алгоритм гістограми напрямлених градієнтів і класифікація методом опорних векторів

Виявлення осіб на зображенні методом гістограми напрямлених градієнтів (HOG) та з допомогою машин опорних векторів (SVM) засновані на принципі ковзного вікна, який можна повністю описати наступним чином.

Спершу розраховується гістограма напрямленого градієнта для всіх зображень об'єктів, підлягають виявлення у навчальній вибірці.

Потім навчається класифікатор SVM на основі цих даних. У процесі виявлення використовується набір вікон, розмір яких фіксований. кожне таке вікно обходить зображення і обчислює HOG для заданою області, а навчений SVM-класифікаторвирішує, чи відносити знайдений об'єкт до шуканого.

Наприкінці цього процесу виходить набір вікон з можливими об'єктами, виключаються лише зайві вікна шляхом злиття вікон з найбільшими перетинами та видалення інших [11].

2.2.4. Ансамбль дерев регресії

Визначення ключових точок обличчя відбувається за допомогою алгоритму, що заснований на ансамблі дерев регресії. Для його навчання потрібні наступні дані:

– навчальний набір помічених вручну ключових точок на зображенні, тобто. конкретний набір (x, y)-координат областей, оточуючих кожну частина особи (рот, око, брова і т.д.);

– задані ймовірності відстаней між парами вхідних пікселів. Ці дані є частиною 68-точкового набору даних iBUG 300-W, на якому відбувалося навчання модуля face_recognition. Існує велика кількість різновидів детекторів ключових точок облич, до прикладу модель зі 194 точок, навчена на наборі тренувальних даних HELEN. Однак 68 ключових характеристик буде цілком достатньо для побудовиточок лиця з високою точністю.

З допомогою перерахованих навчальних даних ансамбль дерев регресії навчається знаходити розташування ключових точок, які будуються по інтенсивностям пікселів.

Реалізація обраного методу детектування характеристик розрахована на пошук 68 ключових точок, представлених на рис. 2.9.

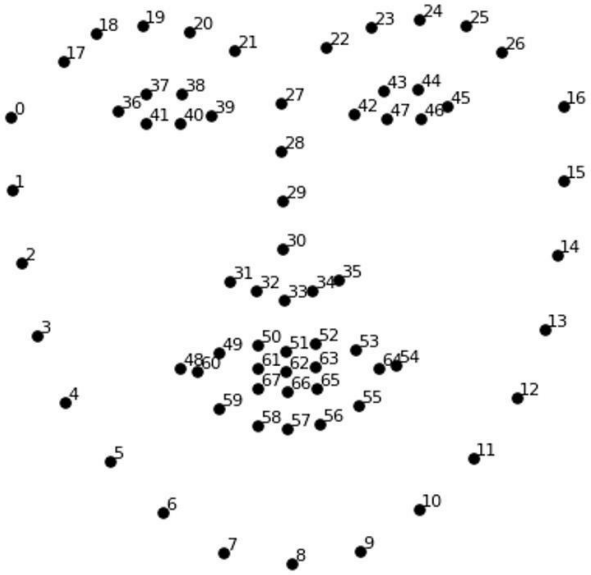

Рис. 2.9. Шаблон 68 ключових точок особи

Завдяки нанесеним на зображення точкам, обличчя можна трансформувати для покращення точності розпізнавання. Для цього будуть використовувати основні перетворення зображення, які зберігають паралельні лінії (афінні перетворення). З їх допомогою зображення трансформується таким чином, щоб очі, рот і ніс розташовувалися максимально по центру. Результат перетворень показано на рис. 2.10.

Рис. 2.10 - Перетворення обличчя

Як показано на рис. 2.10 алгоритм отримує на вхід зображення, по якому будує ключові точки. Потім програма намагається трансформувати зображення так, щоб воно стало максимально схожим з шаблоном, при цьому не змінивши ключові характеристики особи.

2.2.5. Згорткова нейронна мережа (CNN)

У згортковій нейронній мережі реалізовано кілька шарів, які перетворюють вхідні дані у вектор приналежності до класів. Основні шари, які використовуються в згорткової мережі - це шари згортки, шар лінійної ректифікації, шар субдискретизації і повнозв’язний шар. У кожного з них свої функції і завдання, але в результаті виходить складно структурована мережа з найкращими результатами класифікації об'єктів на зображенні [2]. Розглянемо кожен шар більш детально.

Згортковий шар є головним шаром згорткової нейронної мережі. Його основне призначення – виділити ознаки на вхідному зображенні та сформувати карту ознак. Карта ознак – це масив матриць, в якому кожен канал відповідає за певну ознаку [10].

Щоб шар міг виділяти ознаки використовуються фільтри, які також є набором тензорів. Ці тензори мають однаковий розмір, а їхня кількість визначає глибину вихідного 3D масиву. При цьому, глибина самих тензорів збігається з кількістю каналів вхідного зображення.

Вагові коефіцієнти ядра згортки (невеликої матриці) невідомі і встановлюються в процесі навчання.

Фільтр, який застосовується до обробки зображення, не змінюється під час самого проходження і виходить, що число параметрів в багато раз менше, чим у повнозв’язній мережі.

Згортка - процес обчислення нового значення пікселя з врахуванням начень його сусідів. Нижче представлений алгоритм.

Фільтр накладається на ліву верхню частина зображення і здійснюється покомпонентне множення значень фільтра і значень зображення, після чого фільтр

переміщається далі по зображенню до тих пір, поки аналогічним чином не будуть оброблені всі його ділянки.

Потім значення отриманих матриць підсумовуються в єдину матрицю - результат застосування фільтра. Після цього до кожного значення матриці додається однакове число - значення зміщення даного фільтра. Отримана матриця складає один канал вихідний карти ознак.

Після того, як будуть отримані канали для кожного з фільтрів, матриці поєднуються в єдиний тензор, завдяки чому на виході знову виходить зображення, з іншим числом каналів і, можливо, іншим розміром. [10]

Шар активації представляє з себе деяку функцію, яка застосовується до кожному числу вхідного зображення. Традиційно буливикористані функції Sigmoid та Tanh (рис. 2.11).

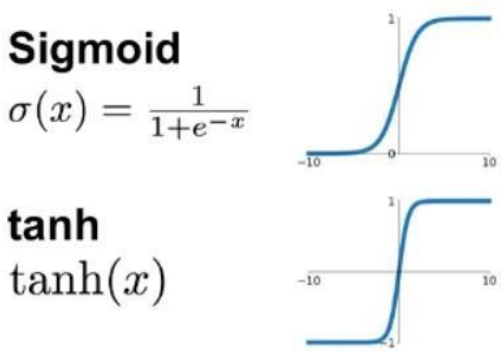

Рис. 2.11. Функції активації

Однак у 2000-х роках було запропоновано та досліджено нову функцію активації - ReLU, яка дозволила суттєво прискорити процеснавчання (рис. 2.12).

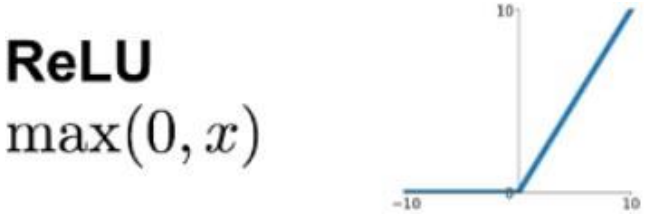

Рис. 2.12. Функція активації ReLU

Наступний етап - це шар підбору (Пулінгу) (рис.2.13.), призначений для зменшення розміру простору ознак, при цьому важлива інформація залишається. Існує кілька версій шару пулінгу, але найбільш поширеною є макспулінг. На рисунку 9 представлено кілька популярних видів шарів пулінгу.

Рис. 2.13 - Види пулінгу

Шар пулінгу має лише один параметр - крок пулінгу. Це значення визначає, на скільки слід зменшити розмірність простору. Шар пулінгу зменшує розмір вхідного тензора вдвічі.

Після кількох етапів згортки та підбору, система перетворюється від конкретної піксельної сітки високої роздільності до більш абстрактних карт ознак. Зазвичай кількість каналів збільшується на кожному наступному етапі, а розмірність зображення у кожному каналі зменшується. У результаті отримується значний набір каналів, які зберігають обмежену кількість даних (навіть один параметр). Ці дані інтерпретуються як абстрактні концепції, виявлені на вихідному зображенні.

Ці дані об'єднуються і передаються в звичайну повнозв'язну нейронну мережу, яка також може складатися з кількох шарів. В теж час повнозв'язкові шари вже втрачають піксельну просторову структуру і мають щодо невелику розмірність (щодо кількості пікселів у вихідному зображенні).

Як і повнозв’язна нейронна мережа, згорткова мережа навчається з допомогою алгоритму зворотного поширення помилки. Спочатку виконується пряме поширення від першого шару до останнього, після чого обчислюється помилка на

вихідному шарі та поширюється назад. При цьому на кожному шарі обчислюються градієнти параметрів навчання, які в кінці зворотного розповсюдження використовуються для оновлення ваг за допомогою градієнтного спуску. [10]

Висновок до розділу 2.

Отже в даному розділі розроблено архітектуру системи розумного будинку з біометричним методом ідентифікації користувачів.

Для розпізнавання облич з відеокамер було прийнято рішення використати:

–гістограма напрямлених градієнтів (HOG) для виявлення особи;

–ансамбль дерев регресії (випадковий ліс) для побудови ключових точок;

–згорткова нейронна мережа (CNN) для обчислення ключових ознак;

–лінійний метод опорних векторів (SVM) для класифікації.

РОЗДІЛ 3
АПРОБАЦІЯ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ В СИСТЕМІ РОЗУМНОГО БУДИНКУ

3.1. Програмна розробка модулів системи ідентифікації осіб по обличчю

Для розробки інтелектуальної системи розпізнавання осіб вибрано мову програмування Python [8]. Вибір здійснено через наявність великої кількості бібліотек і модулів, зручний і зрозумілий синтаксис, а також легку читабельність коду.

Основним інструментом для розпізнавання обличчя є бібліотека face_recognition [15], яку розробив [14] на базі бібліотеки dlib. Обрано цю бібліотеку через її просту реалізацію, використання натренованої нейронної мережі глибокого навчання для обчислення ключових точок, а також використання лінійного методу опорних векторів і гістограми напрямлених градієнтів для виявлення осіб.

Додатково будуть використовуватися наступні бібліотеки:

Модуль Pickle: потужний алгоритм серіалізації і десереалізації об'єктів. Використовуватиметься для створення бази даних імен та «унікальних ознак осіб».

Модуль Os: використовуватиметься для вилучення назв зображень.

Бібліотека OpenCV: містить алгоритми комп'ютерного зору і обробки зображень. Використовуватиметься для захоплення відеопотоку з камери, трансформації зображення та виділення осіб під час процесу розпізнавання.

Бібліотека numpy: додає підтримку багатовимірних масивів і матриць, а також дозволяє проводити обчислення над ними завдяки високорівневим математичним функціям.

Запуск програми буде здійснюватися в інтегрованою середовищі розробки PyCharm, представляючу собою інтелектуальний редактор коду. Дане середовище розробки надає функцію навігації коду, його автодоповнення і інспекції у режимі реального часу.

3.1.1. Реалізація модуля збереження кодувань в файл (data.py).

На початку програми було проведено підключення необхідних бібліотек (рис.3.1)

```
import face_recognition
import pickle
import os
```

Рис.3.1. Підключення бібліотек

Їх функції наступні:

–face_recognition для завантаження зображень та пошуку обличчя та його ключових ознак;

– pickle для створення бази даних;

–os для відділення назви зображення від його формату.

Далі створюється три змінних:

– стрічкова змінна path, що містить назву каталогу, в якому будуть зберігається фотографії людей;

–змінна myList, у яку з допомогою функції os.listdir(path) записується список, що містить імена файлів у каталозі, заданому шляхом path;

–змінна encodeList, яка є словником даних і містить групи значень та пар ключ-значення. Ключами є імена людей, а відповідні кодування їх облич передані до груп значень.

Після оголошення змінних потрібно по черзі завантажити всі фотографії з каталогу, отримати і зберегти їх назви і кодування осібв словник даних.

Для виконання цією цілі був створено цикл for cl inmyList. Усередині циклу зберігається змінна curImg, в яку за допомогою функції load_image_file(f'{path}/{cl}') бібліотеки face_recognition завантажується поточне зображення.

Наступним кроком ми передаємо ім'я файлу та кодування обличчя у словник даних.

Для виконання даної операції ми привласнюємо значенню змінної encodeList результат роботи функції «face_encodings(curImg) [0]». Дана функція приймає зображення і повертає 128-мірний масив, що зберігає кодування особи.

Словник зберігає ключ і групу значень, тому масив кодувань особи буде зберігається в парі з назвоюзображення, з якого було отримано ці кодування. Назва кожного зображення повинна відповідати імені людини, обличчя якої знаходиться в цьому зображенні.

Щоб імена не мали формату зображення (.jpg, .png і тощо) була використана функція splitext модуля os.path. Як вхідний параметр до неї подається назва зображення (cl), а повертається значення - подвійний кортеж (root, ext). Якщо cl починається з точки і містить не більше однієї точки, що повертається ext буде порожнім. У разі зображення, назва якого не містить точок, функція поверне його назву, відкинувши розширення.

Після закінчення циклу заповнюється словник encodeList, який при допомозі бібліотеки pickle буде збережений в вигляді файлу «dataset_faces.dat».

Для цього використовується функція open з атрибутами wb (w – запис, b – бінарний режим). Вона відкриває або створює файл, якщо він не існує, «dataset_faces.dat», в який буде збережений словник encodeList за допомогою функції dump бібліотеки pickle. Dump приймає в себе змінну encodeList і файл «dataset_faces.dat», після чого записує серіалізований об'єкт у файл.

3.1.2. Реалізація модуля розпізнавання осіб (recognition.py)

На початку програмного коду підключаються всі необхідні бібліотеки:

– face_recognition для пошуку осіб на зображенні і вилучення його ключових ознак;

– pickle для завантаження бази даних у програмний код з файлу;

– numpy для пошуку максимального подібності між обличчям з бази даних з обличчям з відеопотоку;

– cv2 для захоплення відеопотоку, трансформації зображень та виділення особи людини в кадрі.

Після оголошення бібліотек оголошуються наступні змінні:

– Method - рядкова змінна, що зберігає в собі назви алгоритму, який буде використовуватися для виявлення осіб на зображенні;

– font - змінна що зберігає в собі шрифт, яким буде написано ім'я людини в процесі розпізнавання;

– frame_skip, що зберігає в собі « *n* « кількість кадрів, що пропускаються. Так як процес розпізнавання осіб вимагає високою обчислювальної потужності було прийнято рішення пропускати кілька кадрів і розпізнавати особи кожен « *n* « кадр;

– imgresize зберігається число від 0 до 1.0. Змінна відповідає за те, на скільки буде стиснуте зображення з відеопотоку;

– scale використовується для обчислення коефіцієнта масштабування рамки особи, так як пошук особи йде на стиснутим зображення, а виділення на оригінальному;

– у FPS слід записати кількість кадрів за секунду, що передає відеокамера;

– у змінну framesPerSecond буде присвоєно обчислене значення кількості кадрів відеопотоку в секунду, що видаються в результаті роботи програми;

– frame_counter що зберігає в собі 0. Ця змінна так само бере участь у обчисленні кількості кадрів в секунду.

Після оголошення змінних потрібно завантажити базу даних в програмний код. Для цього використовується функція open з атрибутами «rb» (r - читання, b – бінарний режим) в яку передається назва файлу бази даних «dataset_faces.dat». Далі змінної all_face_encodings присвоюється результат роботи функції load бібліотеки pickle. Ця функція читає об'єкт з відкритого файлу та повертає зазначену в ньому відновлену ієрархію об'єктів (рис.3.2).

```
        # Завантаження бази даних
        with open("dataset_faces.dat", "rb") as file:
            all_face_encodings = pickle.load(file)
        # Оголошення змінних
        classNames = list(all_face_encodings.keys())
        encodeListKnown = list(all_face_encodings.values())
        # Вказання номеру камери
        cap = cv2.VideoCapture(0)  # 0 - вбудована камера, можна змінити на 1
або інше, якщо є додаткові камери
        # Налаштування параметрів камери
        cap.set(3, 640)  # ширина кадру
        cap.set(4, 480)  # висота кадру
        while True:
            success, img = cap.read()  # Отримання кадру з камери
                # Трансформація зображення
            imgS = cv2.resize(img, (0, 0), None, 0.25, 0.25)
            imgS = cv2.cvtColor(imgS, cv2.COLOR_BGR2RGB)
                # Розпізнавання осіб
            facesCurFrame = face_recognition.face_locations(imgS)
            encodesCurFrame      =      face_recognition.face_encodings(imgS,
facesCurFrame)
            for encodeFace, faceLoc in zip(encodesCurFrame, facesCurFrame):
                # Порівняння обличчя з базою даних
                matches   =   face_recognition.compare_faces(encodeListKnown,
encodeFace)
                faceDis   =   face_recognition.face_distance(encodeListKnown,
encodeFace)
                        # Знаходження найменшого відстані
                matchIndex = np.argmin(faceDis)

                # Вивід імені на відео
                if matches[matchIndex]:
                    name = classNames[matchIndex].upper()
                    y1, x2, y2, x1 = faceLoc
                    y1, x2, y2, x1 = y1 * 4, x2 * 4, y2 * 4, x1 * 4
                    cv2.rectangle(img, (x1, y1), (x2, y2), (0, 255, 0), 2)
                    cv2.putText(img,     name,     (x1,     y1     -     10),
cv2.FONT_HERSHEY_SIMPLEX, 0.9, (0, 255, 0), 2)

            # Показ відеопотоку
            cv2.imshow('Webcam', img)
```

Рис.3.2. Лістинг фрагменту коду модуля розпізнавання осіб

Далі, коли база даних завантажена в програмний код, потрібно оголосити змінні classNames і encodeListKnown. У першу змінну передається перелік імен людей з бази даних при допомоги функції keys().

У другу повертається результат роботи функції values(), яким є двовимірний масив кодувань осіб.

Наступним кроком потрібно вказати програмі з який камери зчитувати відеопотік. Для цього в змінної cap створюється об'єкт VideoCapture(j) бібліотеки openCV, де j - номер підключеної камери. Так ж, при допомоги функції set налаштовуються параметри камери, а саме: кількість пікселів по ширині та висоті.

Наразі всі підготовчі дійства виконані. Наступним рядком оголошується цикл, який буде розпізнавати особу на протягом всієїтрансляції відеопотоку та може бути зупинений кнопкою esc.

На початку циклу змінна frame_counter перевіряється на 0. Якщо оператор if повертає true, створюється змінна time_to_skipping (при наступних ітераціях циклу вона оновлюється), в яку буде записуватися кількість «тиків» з моменту її оголошення, інакше оператор не виконує будь-яких операцій.

Щоб покадрово передавати зображення з камер відеоспостереження використовуватиметься функція read(). Перше значення, що повертається типу Boolean (True чи false) залежно від цього чи правильно врахований кадр, буде записуватись у змінну success. Друге значення повертає саме зображення, яке записується в змінну img.

Наступним кроком зображення трансформується з допомогою алгоритму resize бібліотеки opencv.

Resize має наступні вхідні дані:

–src -зображення для трансформації;

–dst – вхідне зображення, має розміри наступного параметра (dsize), коли він не дорівнює нулю;

–dsize – розмір вхідного зображення (вводиться як кортеж);

–fx – коефіцієнт масштабування горизонтальної осі;

–fy - коефіцієнт масштабування вертикальної осі;

–interpolation – метод інтерполяції.

Уданому випадку алгоритму передається:

–зображення (img); Маніпулювати розміром зображення будуть коефіцієнти масштабування, так що значення переданого кортежу рівні (0,0);

–dst передається «None», так як dsize дорівнює нулю використовувати цей параметр не є можливо;

–fx і fy приймають значення змінної «imgresize».

Таким чином вхідне зображення стискається на 50% по горизонталі і вертикалі. Результат роботи функції записується в змінну imgS.

Порядок цифрових каналів в бібліотеці OpenCV - BGR, однак алгоритми розпізнавання осіб працюють у RGB, тому наступним етапом потрібно його змінити. Найпростіше рішення - використовувати функцію cvtColor, до якої передається зменшене зображення imgS та параметр трансформації cv2.COLOR_BGR2RGB. Повертається значення присвоюється в imgS.

Наступним елементом є умовний оператор if, який перевіряє чи потрібно робити розпізнавання осіб цьому кадрі чи ні. Коли його повертається значення істинно, програма починає пошук осіб і їх ключових ознак на поточному зображення. Для цього використовуються функції з бібліотеки face_recognition.

У функцію face_locations передаються наступні вхідні дані: Перший аргумент - оброблене зображення imgS. Другим аргументом передається рядкова змінна METHOD, у якій зберігається назва методу виявлення осіб «hog». Результат роботи алгоритму записується в змінну FaceFrame.

Іншим алгоритмом є face_encodings, в Котрий передається зображення imgS, а також нещодавно отримані координати розташування особи FaceFrame. Обчислені ключові ознаки особи записуються в змінну encodeFrame.

Настав етап порівняння осіб. У наступному циклі програма порівнює знайдені Характеристики особи з відомими їй і вирішує існує чи ця особа в базі даних чи ні.

Змінні encodeFace та faceLoc отримують значення encodeFrame та FaceFrame відповідно, після для кожного encodeFace і faceLoc відбуваються наступні події.

Спочатку перевіряються бази даних на наявність знайдених на зображенні осіб. На вхід в обидві функції подається двовимірний масив відомих осіб encodeListKnown і нещодавно отримана кодування осіб з відеопотоку encodeFace. Функція compare_faces поверне перелік Boolean значень (True/False), який буде записано до змінної матчі. Вона порівнює кодування осіб з бази даних з особою на зображенні та вирішує,існує воно у базі даних чи ні.

Допустиме відхилення (tolerance) дорівнює 0.6, тобто якщо ключові характеристики особи більш ніж на 60% схожі з відомими - функція повертає True. Однак у таких умовах існує ймовірність знайти одночасно два або більше особи, відповідні за критерієм порівняння.

Щоб цього не допустити було додано алгоритм face_distance. Він виробляє обчислення і повертає в змінну faceDis евклідову відстань між порівнюваним і кожним відомою системою особою. В такому випадку чим менша відстань - тим більше подібність з особою. Щоб знайти мінімальну відстань між характеристиками використовується функція argmin, в яку передається масив faceDis. на виході виходить індекс мінімального елемента, який зберігається в змінну matchIndex.

На наступному етапі потрібно передати знайдені координати осіб faceLoc у координати y1, x2, y2, x1. Оскільки координати були отримані на стиснутим зображенні потрібно масштабувати кожну координату на заздалегідь вирахований коефіцієнт масштабування scale. Далі з допомогою умовного оператора if перевіряється чи існує у базі даних особа з даними індексом.

Якщо особа існує:

– оголошується змінна name, в яку присвоюється ім'я з масиву classNames з індексом matchIndex;

– далі для побудови квадрата, що обводить обличчя на зображенні, використовується функція cv2.rectangle, в яку передаються такі аргументи: зображення, на якому потрібно побудувати прямокутник; координати для побудови; колір прямокутника в форматі BGR; товщина ліній;

– наступним рядком будується прямокутник з допомогою тій ж функції cv2.rectangle з такими координатами, щоб він розташовувався безпосередньо під квадратом, Котрий обводить обличчя. Доданий аргумент cv2.FILLED, Котрий заповнює область прямокутника суцільним кольором.

```
 top, right, bottom, left = faceLoc
cv2.rectangle(imgS, (left, top), (right, bottom), (255, 0, 0), 2)
cv2.putText(imgS, name, (left, top - 10),
cv2.FONT_HERSHEY_SIMPLEX, 0.5, (255, 255, 255), 2)
```

У результаті, якщо дані matches задовольняють обмеження оператора if програма побудує зелений квадрат навколо обличчя і прямокутник того ж кольори безпосередньо під ним.

У випадку, коли особи з таким індексом не існує:

– змінної name присвоюється значення «Unknown»;

– перша та друга функція cv2.rectangle передаються ті ж вхідні параметри за винятком елемента барвисті.

Для виділення невідомої особи використовуватиметься червоний колір прямокутників.

Тепер, коли обличчя виділено, а в змінної name зберігається інформація про ім'я, потрібно вивести текст та розташувати його в області прямокутника, залитого кольором. Висновок тексту відбувається з допомогою функції cv2.putText з наступними аргументами: зображення на яке буде виведений текст; рядок з ім'ям людину; координати на яких повинен розташовуватися текст; шрифт тексту; коефіцієнт, на Котрий множиться базовий розмір шрифту; колір шрифту у форматі BGR; товщина шрифт.

Наступним рядком до змінної frame_counter додається 1. Це потрібно для того, щоб перевірити, чи потрібно розпізнати поточний кадр або ні, а також підрахувати кількість циклів програми. Однак в випадку тривалою роботи програми значення frame_counter можуть перевищувати десятки тисяч, що вплине на її ефективність. Щоб уникнути цієї проблеми існує наступний умовний оператор. Якщо frame_counter дорівнює 30, тоді виконуються наступні дії:

1) Обчислити кількість секунд, витрачених на обробку 30 циклів. Для цього потрібно:

– отримати значення функції cv2.getTickCount, яка поверне поточний час роботи програми;

– відняти з поточного тику змінну time_to_skipping, в якої зберігається час, записаний 30 кадрів назад;

– розділити отриману різниця на частоту тиків, обчислену з допомогою функції cv2.getTickFrequency

2) Вирахувати і записати в framesPerSecond кількість кадрів в секунду відеопотоку, яке змогла обробити програма. Це розраховується розподілом кількості кадрів на секунду, що видається камерою (FPS) на кількість секунд, витрачених на обробку того ж числа циклів програми (time_to_skipping).

Обнулити frame_counter для початку нового відліку.

Виведення кількості кадрів за секунду відбувається за допомогою функції cv2.putText з аргументами:

– зображення, на яке буде виведено текст;

– рядок з кількістю кадрів в секунду; координати на яких повинен розташовуватися текст; шрифт тексту;

– коефіцієнт, на який множиться базовий розмір шрифту;

– колір шрифту в форматі BGR;

– товщина шрифту.

Функція cv2.imshow виводить вікно з зображенням і має два аргументи - назва вікна та зображення, яке слід вивести.

```
# Виведення зображення
    cv2.imshow('Result', imgS)
    # Зупинка при натисканні клавіші 'Esc'
    k = cv2.waitKey(1)
    if k == 27:  # 'Esc'
        break
```

Щоб програма не працювала нескінченно слід додати умову при якому вона буде зупинена. З цією метою оголошується змінна *k* в якій зберігається функція cv2.waitkey, яка чекає натискання якої або кнопки і повертає її значення. Для завершення роботи програми була обрано клавіша «Esc». Оператор if перевіряє, є чи натиснута клавіша «Esc». Якщо умова виконується - цикл програми зупиняється оператором break.

Як тільки нескінченний цикл зупинено слід звільнити камеру функцією release, а також закрити вікно відображення відеопотоку за допомогою cv2.destroyAllWindows на цьому завершується робота модуля розпізнавання осіб.

3.2. Тестування і аналіз результатів

Результатом тестування системи має стати точна відповідність поставленої задачі. Проекту необхідно правильно створювати базу даних кодувань осіб,

розпізнавати відомі особи, а також виявляти невідомі. Опробуємо весь реалізований функціонал розроблених модулів.

Спочатку потрібно створити базу даних кодувань осіб. Для цього в папку з назвою «Resource» потрібно помістити фотографії осіб людей, яких система повинна буде розпізнавати. на рис. 3.3 показано папка «Resource» і її вміст.

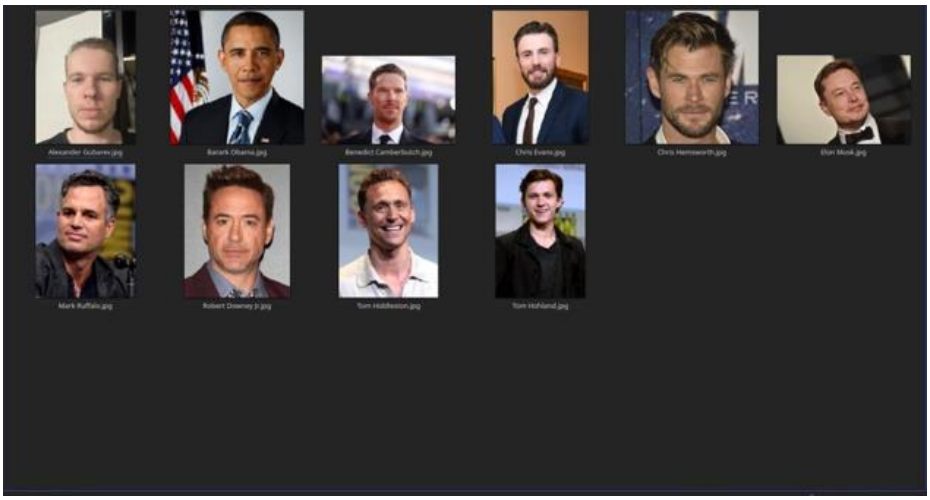

Рис. 3.3. Вміст каталогу «Resource»

Наступним кроком слід запустити програму data.py. З використанням програми PyCharm виконується запуск програми. У результаті було створено файл «dataset_faces.dat», у якому зберігатимуться кодування осіб людей з каталогу «Resource». У результаті роботи

програми, в консолі повинна з'явитися напис про успішному створенніфайлу, а процес завершитися з кодом 0. Запуск програми data.py з допомогою середовища розробки PyCharm показаний на рис. 3.4)

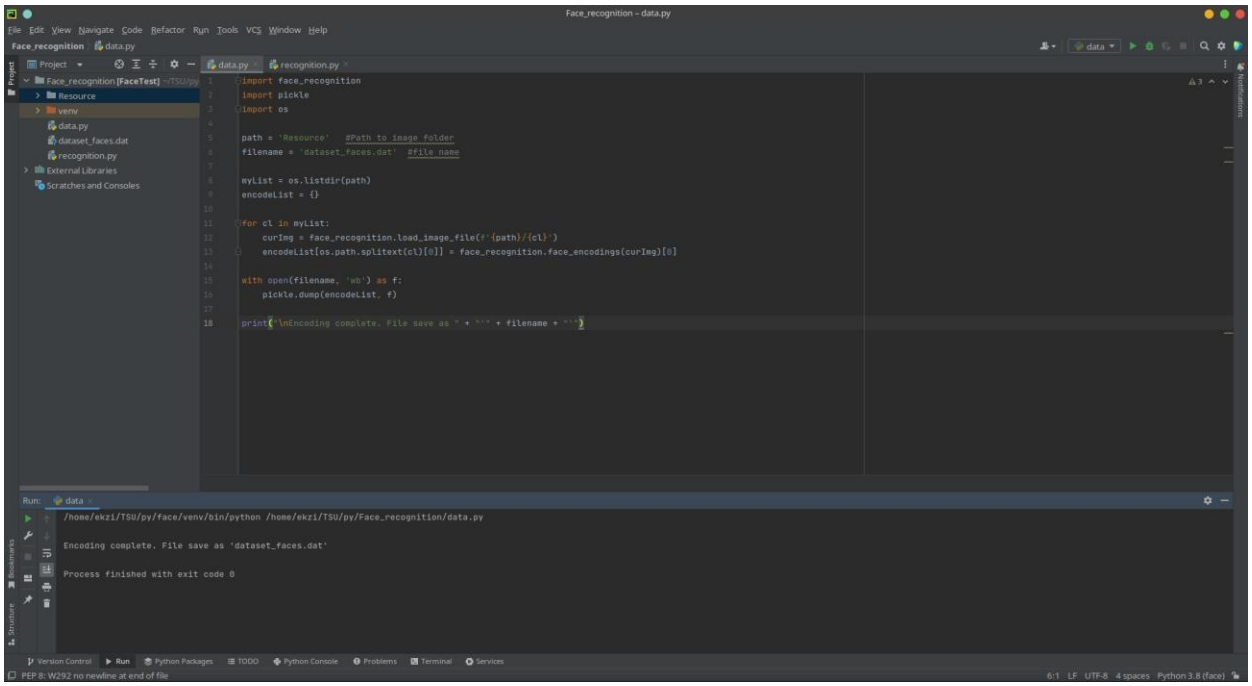

Рис. 3.4. Результат роботи програми

Напис про успішному створенні файлу з'явилася, а програма завершила свою роботу з кодом 0. Тепер можна переконатися в існуванні файлу «dataset_faces.dat», відкривши каталог.

Тепер, коли кодування збережено в окремий файл, можна розпочати розпізнавання осіб. Для цього буде використовуватись програма recognition.py. За допомогою середовища розробки PyCharm виконується запуск програми recognition.py. Результат запуску програми показано на рис. 3.5.

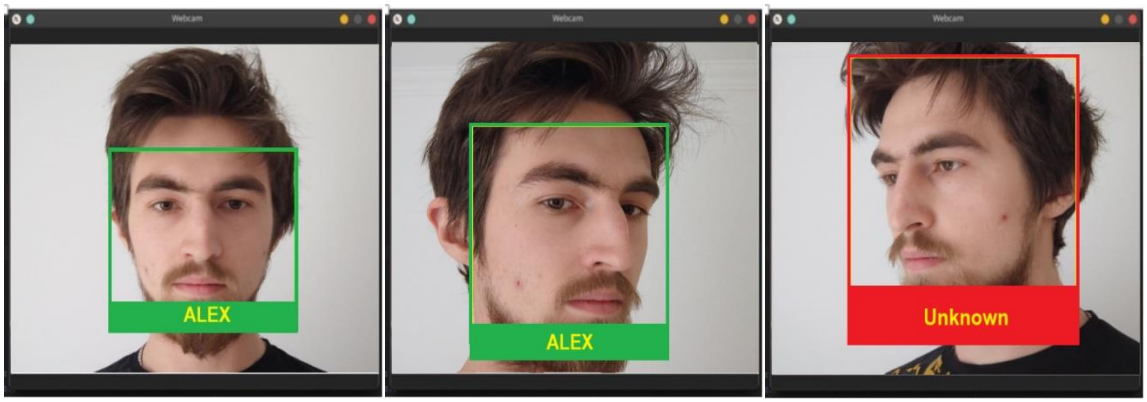

Рис. 3.5. Результат запуску програми «recognition»

Як можна помітити на рис. захоплення відеопотоку з камери пройшло успішно, зображення було оброблено, а обличчя знайдено і розпізнано, проте є помилкові спрацювання, коли лице занадто повернуте відносно камери.

Наступним етапом у тестуванні системи є перевірка пошуку невідомих осіб, а також можливість одночасного виявлення кількох осіб. На рис.3.6, наведено приклад коли в кадрі камери двоє людей, обличчя одного з них відсутнє в базі даних.

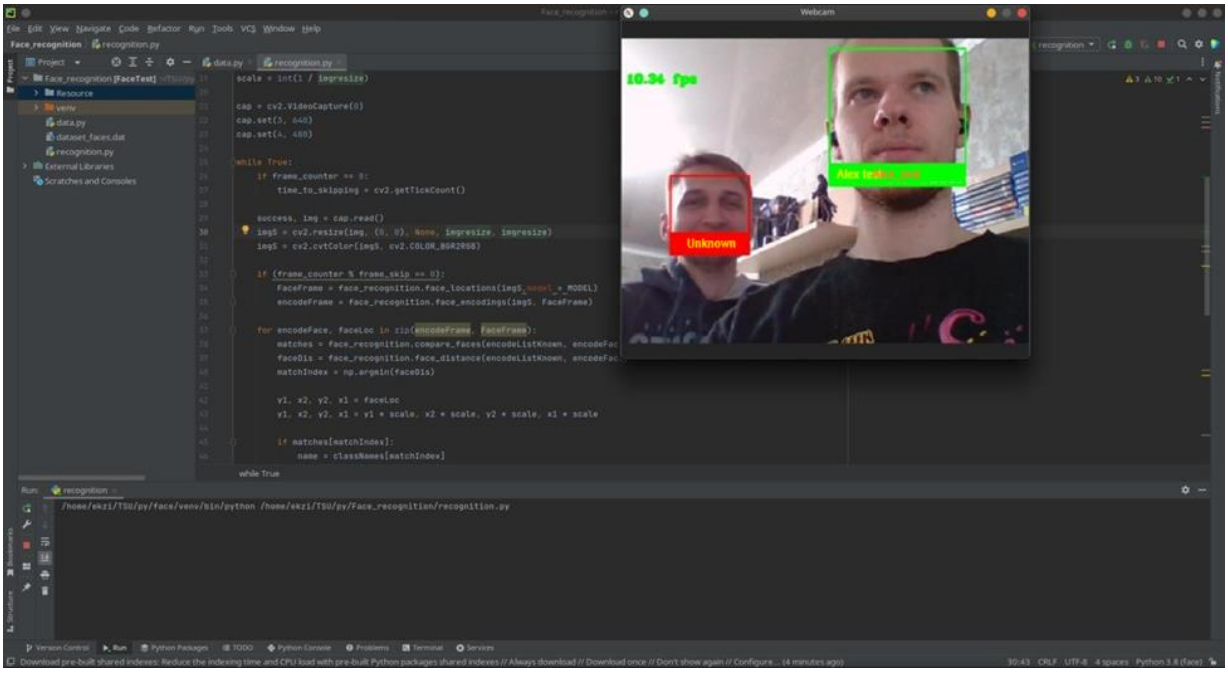

Рис. 3.6. Результат перевірки системи розпізнавати кілька осіб

Після перевірки стає зрозумілим, що програма успішно проводить пошук кількох осіб, а також виявляє і виділяє невідомі їй особи на зображенні.

Висновок по третьому розділу.

Було обрано мову програмування та середовище розробки, описані використовувані бібліотеки і наведено програмна реалізація двох модулів системи розпізнавання осіб:

– перший – модуль збереження відомих кодувань осіб у файл. Цей модуль скорочує час запуску системи розпізнавання, оскільки саме в ньому буде

обчислення кодувань осіб з бази даних;

– другий - модуль розпізнавання осіб, з допомогою якого відбувається зчитування інформації з відеопотоку, трансформація зображення, а також виявлення і розпізнавання осіб в кадр.

З результатів тестування можна зробити висновок: програма успішно пройшла тестування, впоралася з поставленими перед ній завданнями. Це означає, що розроблена система правильно виконує свої функції і готова до використанню для розпізнавання осіб.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

У кваліфікаційній роботі магістра проведені дослідження систем біометричної ідентифікації користувачів розумного будинку. Під час розв'язання задач дослідження, особливо практичної реалізації системи, враховано вимоги з охорони праці і техніки безпеки, пожежної та електробезпеки. Дотримання норм і правил охорони праці є важливим аспектом у контексті дотримання норм організації робочого місця, забезпечення комфортних та зручних умов праці осіб, які беруть участьу процесі, а це вимагає дослідження та дотримання вимог з охорони праці.

В Україні діє ряд нормативних документів, які визначають вимоги і правила щодо використання комп'ютерної техніки, приміщень з екранними пристроями та ін. Основним нормативним документом при використанні комп'ютерної техніки є ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». Він регламентує, що приміщення для експлуатації комп'ютерної техніки повинно розміщуватися в північній або північно-східній частині будівлі. Площа одного робочого місця повинна становити щонайменше 6 $м^2$, об'єм — щонайменше 20 $м^3$, відстань між робочими столами щонайменше 2,5 м у ряду і 1,2 м між рядами. Стіни приміщень потрібно фарбувати у пастельні тони з коефіцієнтом відбиття 0,5-0,6.

Для профілактики загальної втоми і особливо зорового аналізатора важливе значення має організація режиму праці та відпочинку. Загальна тривалість робочого дня не повинна перевищувати 8 год. Частота і тривалістьперерв залежать від типу та інтенсивності виконуваних робіт. Під час робіт, які виконуються з великим навантаженням, рекомендуються перерви на 10-15 хв. через кожну годину, а при неінтенсивній і монотонній роботі — на 10-15 хв. через кожні дві години. Кількість мікропауз (тривалістю до хвилини)потрібно регулювати індивідуально.

Зміст регламентованих перерв може бути різний: виробнича гімнастика (вправи для очей, гімнастика, спрямована на корекцію вимушеної робочої пози, поліпшення венозного кровообігу, часткову дисфункцію рухової активності), альтернативна допоміжна робота, приймання їжі тощо.

Для того, щоб особи, які займаються дослідженням систем біометричної ідентифікації меншою мірою втомлювались і зберігали високий рівень працездатності, потрібно раціонально організовувати їхні робочі місця.

Зокрема, робоче місце має відповідати основним антропометричним даним людини. Крісло або стілець на робочому місці повинні мати висоту сидіння 40-50 см від рівня підлоги, а також відповідний кут нахилу спинки. Монітори потрібно розміщувати на висоті рівня очей (висота від підлоги до нижнього краю екрана має становити 95-100 см) на відстані 60-70 см від оператора (відстань від краю столу — 50-70 см). Кут зору працюючого щодо екрану має дорівнювати 10-20°, але не більше 40°, кут між верхнім краєм монітора і рівнем очей користувача має становити менш як 10°. Найдоцільніше розміщувати екран перпендикулярно до лінії погляду користувача. Кут нахилу екрана по вертикалі має становити 0-30°. З цією метою сучасні монітори комплектують підставкою з поворотним кронштейном, що дає змогу регулювати кут нахилу монітора і горизонтально обертати його навколо вертикальної осі. Висоту екрана від поверхні підлоги регулюють змінюючи висоту робочої поверхні столу. Іноді монітори встановлюють на спеціальні підставки, що уможливлює його переміщення у просторі у вертикальному та горизонтальному напрямах.

У приміщеннях, де виконуються роботи на ПК, повинно бути передбачене природне і загальне штучне освітлення. Робочі місця користувачів потрібно розміщувати так, щоб у поле зору не потрапляли вікна і освітлювальні прилади (монітори потрібно розміщувати під кутом 90-105° до вікон і на відстані 2,5-4 м від стін і віконних прорізів). У поле зору користувача не повинні потрапляти поверхні, що відбивають світло. Покриття столу має бути матовою з коефіцієнтом відбиття 0,25-0,4.

Для штучного освітлення приміщення рекомендується застосовувати світильники матового світла з розсіювачами, а спектральний склад ламп має наближатися до спектру сонячного світла (наприклад, люмінесцентні типу ЛБ). Оптимальна освітленість робочих місць — 400-500 лк.

При дослідженні та розробці методів біометричної ідентифікації користувачів розумного будинку було дотримано усіх вище наведених вимог нормативних документів щодо охорони праці і техніки безпеки при експлуатації комп'ютерної техніки.

4.2. Безпека в надзвичайних ситуаціях

4.2.1. Організація оповіщення та зв'язку у надзвичайних ситуаціях техногенного та природного характеру

Оповіщення – доведення сигналів і повідомлень органів управління цивільного захисту про загрозу та виникнення надзвичайних ситуацій, аварій, катастроф, пожеж, епідемій тощо до центральних і місцевих органів виконавчої влади (керівників об'єднаних територіальних громад), підприємств, установ, організацій та населення.

Оповіщення здійснюється на рівнях:

–загальнодержавному – оперативно-черговою службою на пункті управління ДСНС;

–територіальному – оперативно-черговими службами на пунктах управління обласних, міських держадміністрацій;

–місцевому – черговими службами місцевих органів виконавчої влади;

–об'єктовому – диспетчерськими (черговими) службами об'єктів, на яких створено спеціальні, локальні та об'єктові системи оповіщення.

З метою створення умов для побудови в Україні автоматизованої системи централізованого оповіщення нового покоління, яка б відповідала сучасним світовим стандартам, Урядом прийнято рішення щодо вдосконалення нормативно-правової бази у сфері організації оповіщення про загрозу виникнення або

виникнення НС і привести її у відповідність до чинного законодавства. Постановою Кабінету Міністрів України від 27 вересня 2017 року № 733 затверджено Положення з організації оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту.

Положення визначає порядок організації оповіщення, забезпечення функціонування апаратури і технічних засобів оповіщення та технічних засобів телекомунікацій.

Керівники всіх рангів зобов'язані встановлювати у населених пунктах, на підприємствах сигнально – гучномовні пристрої, електронні інформаційні табло, радіотрансляційні точки для передачі інформації з питань цивільного захисту.

Системи оповіщення (програмно-технічні комплекси) за рівнями поділяються на: загальнодержавну, територіальну, місцеву автоматизовані системи, спеціальну, локальну, об'єктову системи оповіщення.

Система оповіщення це комплекс організаційно-технічних заходів, апаратури і технічних засобів оповіщення, апаратури, засобів та каналів зв’язку, призначених для своєчасного доведення сигналів та інформації про виникнення надзвичайних ситуацій до центральних та місцевих органів виконавчої влади.

Організація та забезпечення оповіщення про загрозу у надзвичайних ситуаціях здійснюється через:

–ПАТ «Національна суспільна телерадіокомпанія України»;

–державні, публічні, комунальні, громадські телерадіокомпанії;

–операторів телекомунікаційних мереж загального користування;

–Інтернет-ресурси (сайти, соціальні мережі).

4.2.2. Шум, вібрація, ультразвук, електромагнітні випромінювання у виробничих приміщеннях для роботи з ВДТ та захист від них

Під шумом розуміють набір багаточисельних звуків, які швидко змінюються за частотою, силою і складаються з ряду гармонік. Шум є загально-біологічним подразником, що діє не тільки на органи слуху, але може викликати порушення роботи серцево-судинної і нервової систем, зумовлювати професійні захворювання.

Основними характеристиками звукових коливань є інтенсивність (сила), частота і форма звукової хвилі. Інтенсивність визначається енергією, що переноситься за 1 с звуковою хвилею через поверхню площею 1 $м^2$, яка перпендикулярна напрямку розповсюдження звукової хвилі. Одиниця вимірювання – $Вт/м^2$.

Гранично-допустимі рівні шумів санітарними нормами встановлені для кожного класу:

− для високочастотних шумів (вище 800 Гц) – 75-85 дБ;

− для середньо частотних шумів (300-800 Гц) – 85-90 дБ;

− для низькочастотних шумів (до 300 Гц) – 90-100 дБ.

З розвитком промисловості все більший контингент людей підпадає під вплив вібрацій, які являють собою механічні коливання, що передаються тілу людини. Основні параметри вібрацій – частота і амплітуда коливань, але на відміну від шуму, при якому енергія механічних коливань передається через повітряне середовище, при дії вібрацій вона розповсюджується по тканинах і викликає їх коливання або тіла людини в цілому.

Найбільш небезпечна вібрація частотою 16-250 Гц, дія якої призводить до вібраційної хвороби. Нормування шуму здійснюється згідно з «Санітарними нормами допустимих рівнів шуму на робочих місцях».

Для запобігання шкідливої дії шуму і вібрації на організм працюючих проводяться технічні, організаційні і медико-профілактичні заходи. Одним з основних технічних заходів є зменшення при експлуатації та на стадії проектування, конструювання обладнання причин шуму і вібрації в самому джерелі утворення. Якщо неможливо ізолювати чи знизити шум і вібрацію самого джерела, потрібно:

− ізолювати джерело шуму або вібрації від навколишнього середовища засобами вібро- та звукоізоляції;

− раціонально планувати виробничі приміщення, що мають інтенсивні джерела шуму;

− збільшувати звукопоглинання внутрішніх поверхонь приміщення шляхом звукопоглинальних покриттів.

Електромагнітне випромінювання – взаємопов'язані коливання електричного і магнітного полів, що утворюють електромагнітне поле а також, процес утворення вільного електромагнітного поля за нерівномірного руху та взаємодії електричних зарядів. Розповсюдження випромінення здійснюється за допомогою електромагнітних хвиль.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту. Для захисту очей доцільно використовувати захисні окуляри ЗП5-90.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Можна зробити висновок про те, що організація оповіщення та зв'язку у надзвичайних ситуаціях є ключовим елементом системи безпеки. Ефективність цих систем визначається комплексністю, швидкістю та доступністю інформації, а також готовністю населення та служб реагувати на потенційні загрози.

Що стосується забезпечення безпечних та комфортних умов праці з ВДТ у виробничих приміщеннях, то важливо проводити регулярні оцінки шуму, вібрації, ультразвуку та електромагнітного випромінювання, вживати відповідні заходи захисту та дотримуватися нормативів безпеки.

ВИСНОВКИ

Біометрична ідентифікація користувачів в системі розумного будинку визначається високою актуальністю та потенційним впливом на забезпечення безпеки, комфорту та ефективності в повсякденному житті. Результати проведених досліджень в цій роботі можуть бути узагальнені наступним чином:

1.Підбір оптимальних біометричних характеристик: Виконаний аналіз методів біометричної ідентифікації дозволив вибрати оптимальні характеристики для використання в системі ідентифікації користувачів розумного будинку.

2.Проектування структури системи: Була розроблена структура системи біометричної ідентифікації, враховуючи принципи організації системи розумного будинку.

3.Вибір оптимального принципу організації системи розумного: Були обґрунтовані та вибрані оптимальні принципи організаційної структури системи розумного будинку для впровадження біометричної ідентифікації користувачів.

4.Біометричний метод ідентифікації за обличчям: Детально розглянуто біометричний метод ідентифікації особи за особливостями її обличчя. Здійснено вибір алгоритмів та методів обробки зображень для ефективної ідентифікації осіб за ознаками обличчя.

5.Програмна реалізація: Реалізовано механізм ідентифікації користувача в системі розумного будинку на основі розпізнавання обличчя з використанням обраного алгоритму.

6.Практичне тестування: Система розпізнавання облич пройшла успішне практичне тестування, підтверджуючи правильність та ефективність розробленого механізму ідентифікації.

Отримані результати можуть бути корисними для розробників систем розумного будинку та фахівців у галузі біометричних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mikhailov M.A., Volevodz A.G., Sidorenko E.L. Improving the System of Fingerprint Registration // International Scientific and Practical Conference in the State Duma “Improving the System of Fingerprint Registration”. 2016. С. 368-378.

2. Kubitovich S.N. DNK kak nositel informatsii neogranichennogo kruga lits // Vestnik ekonomicheskoy bezopasnosti. 2017. С. 184—188.

3. Edson, A. M. AAMVA Standards Working Group. AAMVA Standard for the Driver License // Identification Card 2000. Technical Report AAMVA DL/ID2000, The American Association of Motor Vehicles Administrators. 2000. С. 1-7.

4. Jain, A. K. Biometrics: Personal Identification in networked Society. // Kluwer Academic Publishers, Boston, MA. 1999. С. 1-9.

5. Anwar, A. S. Human Ear Recognition Using Geometrical Features Extraction. // International Conference on Communication, Management and Information Technology. 2015. С. 531-537.

6. Bradsky, G. Learning OpenCV: Computer Vision with OpenCV Library / G. Bradsky, A. Kaehler. – O'Reilly Media, 2008. – 555 p

7. Histograms of Oriented Gradients for Human Detection Navneet Dalal and Bill Triggs INRIA Rhone-Alps,

8. Талапчук, Сніжана Іванівна. Метод та підсистема ідентифікації користувача кіберфізичної системи “Розумний будинок”. 2023.

9. Lu, H. Calculate Deep Convolution NeurAl Network on Cell Unit/ Haofang Lu, Ying Zhou, Zi-Ke Zhang – Springer Singapore, 2017 – 526 p

10.Rupesh K Srivastava, Klaus Greff, and J¨urgen Schmidhuber. Training very deep networks. In Advances in neural information processing systems, pages 2377–2385, 2015.

11.Dwivedi D. Face recognition for beginers. 2018. URL: https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2 (дата звернення: 12.12.2023).

12.Geitgey A. Face recognition. 2017 URL: https://facerecognition.readthedocs.io/en/latest/readme.html (дата звернення: 12.12.2023).

13.Rovai M. Real-Time Face Recognition: An End-To-End Project. 2018. URL: https://towardsdatascience.com/real-time-face-recognition-an-end-toend-project-b738bb0f7348 (дата звернення: 12.12.2023).

14.Adam Geitgey Deep Learning: Face Recognition https://www.linkedin.com/learning/deep-learning-face-recognition (дата звернення: 12.12.2023).

15.Rosebrock A. OpenCV EigenFaces for face recognition. 2021. URL: https://pyimagesearch.com/2021/05/10/opencv-eigenfaces-for-face-recognition/ (дата звернення: 12.12.2023)

16.Sanjeevkumar A., Suvarna N. Human Identification using Histogram of Oriented Gradients (HOG) and Non-Maximum Suppression (NMS) for ATM Video Surveillance. 2021. 10 с.

17.Кольбух Ю.О. Комп’ютеризована система для керування «розумними» приладами в будинку: кваліфікаційна робота бакалавра за спеціальністю «123 — Комп’ютерна інженерія» / Кольбух Юрій Олегович – Тернопіль, ТНТУ, 2022 – 67с.

18.Козак В. С. Комп'ютерна система керування розумним будинком на основі динамічних користувацьких профілів // Кваліфікаційна робота на здобуття освітнього ступеня бакалавр // ТНТУ, спеціальність 123 «Комп’ютерна інженерія» // Тернопіль, 2022 // с.– 78

19.Чайковський А.В., Жаровський Р.О., Лещишин Ю.З Конспект лекцій з дисципліни «Дослідження і проєктування комп’ютерних систем та мереж» для студентів спеціальності 123 - Комп’ютерна інженерія. Тернопіль, 2021. 148 с.

20.Жаровський, Р. О. Конспект лекцій з дисципліни Захист інформації у комп’ютерних системах. 2019. 268 с.

21. Подвисоцький О., Стадник Н. Методи розпізнавання облич в сситемах ідентифікації користувачів розумного будинку. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана

Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С.98

22. Подвисоцький О., Стадник Н. Методи біометричної ідентифікації в розумному будинку. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 435.

23.Лупенко С.А., Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. 2021. 34 с.

24.Санітарно-гігієнічні норми. Виробничий шум та вібрація. URL: https://www.sop.com.ua/article/193- virobnichiy-shum-ta-vbratsya (дата звернення: 12.12.23)

25.Безпека праці та промислова санітарія. URL: https://cpo.stu.cn.ua/ posibnik/780.html (дата звернення: 12.12.23)

26.Стадник І.Я. Зварич Н.М. Оцінка хімічної обстановки при аваріях на хімічно небезпечних об'єктах з викидом (виливом) небезпечних хімічних речовин та застосуванні хімічної зброї. ТНТУ. 2020. 36 с

Додаток А.

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів
6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

УДК 004.852

О. Є. Подвисоцький; Н. Б. Стадник, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ В РОЗУМНОМУ БУДИНКУ

O. E. Podvysotskyi; N. B. Stadnyk, Ph.D.

METHODS OF BIOMETRIC IDENTIFICATION IN SMART HOME

Біометрична ідентифікація набуває все більшої популярності в сфері розумних будинків. Використовуючи цей метод, користувачі можуть безпечно отримати доступ до своїх осель шляхом простого сканування відбитків пальців, розпізнавання обличчя або голосу. Ця технологія змінює наше сприйняття взаємодії з оточуючим середовищем, забезпечуючи значно вищий рівень безпеки та зручності [1].

Біометрична автентифікація - це метод ідентифікації, який базується на фізичних характеристиках людини, таких як відбитки пальців або риси обличчя, для перевірки особи. Цей метод також може застосовуватися для моніторингу та контролю доступу до приватних зон, таких як житлові будинки чи підприємства.

Розумні будинки мають численні переваги, включаючи зручність, енергоефективність та вищий рівень безпеки. Біометрична автентифікація відіграє важливу роль у забезпеченні високого рівня безпеки та захисту мешканців таких інтелектуальних будинків. Біометричну автентифікацію можна використовувати для захисту доступу до дверей, ліфтів та інших частин будинку, для створення безпечного середовища для мешканців і відвідувачів.

Останнім трендом у біометричній автентифікації є використання штучного інтелекту (ШІ) та машинного навчання [2]. Ці технології використовуються для підвищення точності та швидкості процесу біометричної автентифікації.

Розумні будинки все частіше використовують технологію розпізнавання обличчя як форму біометричної автентифікації - метод перевірки особистості людини шляхом розпізнавання та аналізу її унікальних фізичних характеристик. Розпізнавання обличчя у розумних будинках [3], забезпечує власникам безпечний доступ до своїх осель без необхідності фізичних ключів чи паролів. Крім того, цю технологію можна використовувати для виявлення зловмисників і попередження власників будинків про можливі загрози безпеці.

Технологія біометричної автентифікації все ще розвивається, і є ряд проблем, які треба вирішити, перш ніж її широко застосують. Серед цих питань - точність, конфіденційність та безпека даних, а також необхідність створення єдиного стандарту біометричної автентифікації для різних місць і систем. Тим не менш, потенціал біометричної автентифікації для підвищення безпеки у розумних будинках є значущим. Загалом, впровадження цієї технології може стати корисним інструментом для підвищення безпеки та зручності, однак важливо бути усвідомленим щодо потенційних проблем, пов'язаних із її застосуванням.

Література

1. Noh, Nor Syazwani Md, et al. "Smart Home with Biometric System Recognition." *Journal of Physics: Conference Series*. Vol. 1529. No. 4. IOP Publishing, 2020.

2. Sayyad, Sohel, et al. Smart Home Surveillance System Using Artificial Intelligence. In: *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*. IEEE, 2023. p. 1-7.

3. Rahim, Asif, et al. "Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models." *Sensors* 23.15 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.852
О.Є. Подвисоцький; Н.Б. Стадник, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ РОЗПІЗНАВАННЯ ОБЛИЧЬ В СИСТЕМАХ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ РОЗУМНОГО БУДИНКУ

O.E. Podvysotskyi; N.B. Stadnyk, Ph.D.

METHODS OF FACE RECOGNITION IN SMART HOUSE USER IDENTIFICATION SYSTEMS

У даній роботі вирішуватиметься завдання ідентифікації людей за біометричними даними особи. Будь-який алгоритм ідентифікації осіб повинен вирішувати завдання локалізації особи на зображенні, його нормалізації, обчислення ключових ознак і класифікацію. В якості однієї з таких біометричних ознак є людське обличчя.

Для вирішення завдання необхідно ідентифікувати людину за біометричними ознаками особи на вхідному зображенні. Щоб ідентифікувати людину потрібно, щоб була заздалегідь підготовлена база даних із зображень з людьми, яких потрібно ідентифікувати на вхідному зображенні. На виході повинно виводитися оброблене вхідне зображення, на якому виділено особу людини і є підпис з прізвищем цієї людини, або якщо на вхідному зображення немає людини з бази даних, то повинен виводитися напис, що попереджає про те, що дана людина не ідентифікована. І по результатах ідентифікації може здійснюватись не лише допуск особи, але й налаштування систем розумного будинку.

Фактично завдання ідентифікації людей за біометричними даними особи можна звести до класифікації. Потрібно буде на зображенні знайти обличчя, а також його біометричні ознаки такі як положення очей. Ця біометрична ознака дозволяє більш точно ідентифікувати людину.

Насамперед потрібно локалізувати розташування особи на зображенні. Для цього, існує кілька способів, у цій роботі буде використаний метод Віоли-Джонса, який використовує каскади Хаара. Порівняно з іншими методами, метод Віоли-Джонса досить точний і швидкий. Для більш точної локалізації обличчя на вхідне зображення зображення потрібно перетворити на сірий колір. Далі з допомогою каскадів Хаара визначаємо локалізацію обличчя зображення. Це необхідно для точного знаходження такого біометричного ознаки як розташування очей, а також для більш точної ідентифікації обличчя.

Наступним кроком буде локалізація положення очей. Положення очей є однією з біометричних ознак особи людини, і саме тому в даній роботі положення очей буде використовуватись як біометрична ознака особи людини, для кращої ідентифікації людини.

Наступним кроком необхідно здійснити тренування системи розпізнавання за зібраними ознаками для самої ідентифікації людини. Система розпізнавання навчається на наданій їй базі даних людей, що складаються з зображень з людьми, яких і слід ідентифікувати. За допомогою попереднього навчання раніше система під час надходження вхідного зображення відбувається розпізнання цього зображення та порівняння із зображеннями, які завантажені в систему, і при достатньому збігу ознак на зображенні виводитися id, яке в нашому випадку є прізвищем людини. Якщо збігу не відбулося виводитися напис що означає, що даної людини немає в базі даних.

Для вирішення задач класифікації сьогодні найбільш актуальні методи, засновані на машинному навчанні, оскільки вони показують найкращі результати. Саме тому в цій роботі вони будуть використані.