

КВАЛІФІКАЦІЙНА РОБОТА

магістр
Освітній рівень

Метод автоматизованого керування реєстрацією людей у приміщенні
Назва теми

КвРАКІТР.2023168.01.01 ПЗ

Галузь знань 17 «Електроніка, автоматизація та електронні комунікації»
Шифр, назва

Спеціальність 174 «Автоматизація, комп'ютерно-інтегровані технології та
робототехніка»
Шифр, назва

Освітня програма «Автоматизація, комп'ютерно-інтегровані технології та
робототехніка»
Назва

Виконав:

студент ІІ курсу, група АКІТРм-23-1 
Підпис

Владислав АНТОНІЮК
Ім'я, ПРІЗВИЩЕ

Керівник


Підпис, дата

Юрій ФОРКУН
Ім'я, ПРІЗВИЩЕ

Нормоконтролер


Підпис, дата

Людмила КОРЕЦЬКА
Ім'я, ПРІЗВИЩЕ

До захисту допускаю:
зав. кафедри АКІТтаР


Підпис, дата

Валерій МАРТИНЮК
Ім'я, ПРІЗВИЩЕ

«20» грудня 2024 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

Рівень вищої освіти другий (магістерський)

Галузь знань 17 – Електроніка, автоматизація та електронні комунікації

Спеціальність 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка

Освітня програма Автоматизація, комп'ютерно-інтегровані технології та робототехніка

ЗАТВЕРДЖУЮ

Завідувач кафедри АКИТтаР

Валерій МАРТИНЮК

01 вересня 2024р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Антошку Владиславу Руслановичу

Прізвище, ім'я, по батькові студента

1 Тема роботи Метод автоматизованого керування реєстрацією людей у приміщенні

Керівник роботи Форкун Юрій Вікторович, к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, учене звання

Затверджено наказом ректора університету від 26.08.2024 р. №60

2 Строк подання студентом роботи на кафедру 02.12.2024р.





3 Вихідні дані до роботи Аналіз існуючих у світі класів систем контролю та управління доступом. Розробка алгоритмічного та програмного забезпечення

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ. Дослідження систем контролю та керування доступом. Розробка моделі автоматизації систем контролю та керування доступом. Моделі автоматизованого навчання задач розпізнавання обличчя. Оптимізація частини СККД пошуку. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
презентаційні матеріали (слайди)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Антиплагіат	Федула М.В., доцент кафедри АКИТтаР		
Нормоконтроль	Корецька Л.О., доцент кафедри АКИТтаР		

7 Дата видачі завдання 01 вересня 2024р.

КАЛЕНДАРНИЙ ПЛАН

Назва розділу кваліфікаційної роботи	Строк виконання	Примітка
1 Вступ	10.09.2024р.	Виконано
2 Огляд літературних джерел та патентних даних	25.09.2024р.	Виконано
3 Огляд існуючих моделей	15.10.2024р.	Виконано
4 Розробка моделі автоматизованого навчання задач розпізнавання обличчя	30.10.2024р.	Виконано
5 Розробка програмного забезпечення	10.11.2024р.	Виконано
6 Висновки	15.11.2024р.	Виконано
7 Оформлення пояснювальної записки до кваліфікаційної роботи	20.11.2024р.	Виконано
8 Оформлення презентаційних матеріалів	1.12.2024р.	Виконано

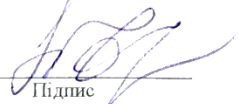
Студент


Підпис

Владислав АНТОНЮК

Ім'я, прізвище

Керівник роботи


Підпис

Юрій ФОРКУН

Ім'я, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод автоматизованого керування реєстрацією людей у приміщенні».

Автор роботи: Антонюк Владислав Русланович.

Керівник роботи: Форкун Юрій Вікторович, к.т.н., доцент

Пояснювальна записка: 85 с., 30 рис., 2 табл., 1 дод., 71 джерело.

Графічна частина: презентаційні слайди.

КОНТРОЛЬ, НАДІЙНІСТЬ, АВТОМАТИЗОВАНА СИСТЕМА,
РЕЄСТРАЦІЯ ДОСТУПУ.

Мета роботи: розробити метод автоматизованого керування реєстрацією людей у приміщенні. Для досягнення поставленої мети вирішено наступні завдання. Спочатку розглядаються існуючі у світі класи систем контролю та управління доступом. Типи доступних систем розпізнавання були вивчені за допомогою діагностичного дослідження, щоб виявити їхні переваги та недоліки. Було вивчено основні інструменти розробки, відібрано найкращі. Існуючі методики розпізнавання облич задокументовані та обговорені. Для читача представлено класифікацію алгоритмів розпізнавання обличчя. Впроваджено програмну систему для створення системи контролю доступу на основі розпізнавання обличчя. Результатом дослідження є автоматизована система контролю та управління доступом, розроблена для системи входу на основі розпізнавання обличчя.



Підпис студента

02.12.2024

Дата

ЗМІСТ

Зміст.....	2
ВСТУП.....	4
1 ДОСЛІДЖЕННЯ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ	6
1.1. Загальні відомості.....	6
1.2 Класифікація СККД.....	7
1.2.1 Системи що знаходяться у мережі СККД.....	7
1.2.2 Системи що не знаходяться у мережі СККД.....	9
1.3. Сучасний стан систем СККД.....	10
1.4 Аналіз систем СККД як об'єкту автоматизованого керування.....	14
1.4.1 Пристрої загрози.....	14
1.4.2. Засоби ідентифікації.....	15
1.4.3 Засоби контролю.....	16
1.4.4 Засоби зчитування.....	16
1.5. Постановка задачі досліджень.....	17
1.6 Висновки до першого розділу.....	18
2 РОЗРОБКА МОДЕЛІ АВТОМАТИЗАЦІЇ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ.....	19
2.1 Опис характеристик керування.....	19
2.2 Обрання платформи для створення локальної системи автоматизації.....	20
2.3. Проектування застосунку.....	24
2.4 Обрання бази даних.....	31
2.5 Монтажно-комутаційна схема автоматизації СККД.....	34
2.5 Висновки до другого розділу.....	37
3 МОДЕЛІ АВТОМАТИЗОВАНОГО НАВЧАННЯ ЗАДАЧ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ.....	38
3.1 Аналіз готових рішень.....	38
3.2 Архітектурні особливості нейромережі FaceNet.....	43

3.3 Аналіз поняття баз даних.....	48
3.4 Висновки до третього розділу.....	55
4 ОПТИМІЗАЦІЯ ЧАСТИНИ СККД ПОШУКУ.....	56
4.1. Робота із векторами даних FaceNet.....	56
4.2 Кластеризація векторів.....	59
4.3 Дослідження роботи підходу до оптимального пошуку.....	65
4.4 Синтезування регулятора для СККД.....	71
4.5 Розробка DFD діаграми.....	72
4.6 Висновки до четвертого розділу.....	74
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	77
ДОДАТОК А Стаття у фаховому журналі.....	85

ВСТУП

Завдання спрямоване на вирішення прикладної задачі, а саме створення системи контролю доступу. Це, звичайно, буде пріоритетом для цього завдання, оскільки проблема безпеки, як особистої, так і громадської, є першочерговою. Опис різноманітних подібних систем, що існують і діють на даний момент, має свої особливості застосування.

Перший служить для опису того, що може робити дана система, а також рівня точності, простоти використання для користувача та здатності обробляти особисті дані, оскільки ці три параметри є найсильнішими і безпосередньо впливають на підвищення або погіршення кінцевої ефективності системи, що розробляється.

На даний момент більшість фірм вже використовують свої системи безпеки – СКУД. Нарешті, впровадження біометричних систем ідентифікації на підприємстві може гарантувати помітне покращення безпеки компанії та її персоналу. Оскільки корпоративний попит на біометричні системи розпізнавання зростає прискореними темпами, технологія розпізнавання обличчя неминуче приверне до себе більший інтерес у найближчому майбутньому.

Мета роботи розробити метод автоматизованого керування.

Об'єкт дослідження: процеси реєстрації реєстрацією людей у приміщенні із обмеженим доступом.

Предмет дослідження метод, засоби та математичні моделі автоматизованого керування реєстрацією людей у приміщенні.

Завдання що вирішуються в роботі:

- розглянути існуючі у світі класи систем контролю та управління доступом;

- дослідити типи доступних систем розпізнавання були вивчити за допомогою діагностичного дослідження, щоб виявити їхні переваги та недоліки;
- вивчити основні інструменти розробки та відібрати найкращі;
- проаналізувати існуючі методики розпізнавання обличь;
- розробити метод, засоби та математичні моделі автоматизованого керування реєстрацією людей у приміщенні;
- розробити програмну реалізацію для створення системи контролю доступу на основі розпізнавання обличчя.

Наукова новизна полягає у розробці методу автоматизованого керування, що покращило точність та швидкість розпізнавання людей у приміщеннях з обмеженим доступом.

1 ДОСЛІДЖЕННЯ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ

1.1. Загальні відомості

У 21 столітті постає проблема встановлення охорони приватної території і взагалі майна, важливих об'єктів тощо. Проблема стала настільки серйозною. Тому що якщо їхні дані або об'єкти будуть доступні неавторизованим особам, результати можуть бути кардинальними. Врешті-решт було прийнято рішення практично по-новому підійти до вирішення питання контролю доступу. Це саме те, що люди пропонували дуже довго. Були спроби випробувати різні підходи; наприклад, рішення, засновані на зчитуванні магнітної смуги або чіпа, можуть бути безпечними порівняно з рішенням, заснованим лише на зчитуванні магнітної смуги, але впровадження безпечного рішення на основі зчитування чіпа є дорогим, повільним і складним. З іншого боку, рішення на основі чіп-карти також критикують через те, що воно зберігає велику кількість персональних даних і не дозволяє користувачам контролювати свої дані, магнітні картки з обмеженим використанням і так далі. Як наслідок, зараз, коли загальна тенденція ідентифікації обличчя почала поширюватися, за належного підходу цей тип контролю та управління доступом можна вважати найефективнішим рішенням для захисту людей.

Система контролю та управління доступом (СКУД) — це набір засобів, як апаратних, так і програмних, призначених для обмеження доступу до об'єкта та фіксації використовуваних точок доступу. Основним завданням АССУ є обмеження доступу до конкретної території (об'єкта) та реєстрація використовуваних точок доступу.

— контроль доступу та обмеження до певної зони — дозволить вам визначити правила у визначеній зоні щодо того, хто, коли та якою мірою має доступ до цього місця. Надалі правила можна використовувати для розподілу

обов'язків і визначення особливостей об'єкта, який потребує підвищеної безпеки.

– визначити, хто має доступ до певної області — це може бути важливою інформацією для відстеження пов'язаних робочих годин і будь-яких проблем, що виникають.

Інші обов'язки:

– облік відпрацьованого часу: це також включає керування базами даних для персоналу та відвідувачів;

– інтеграція з системою безпеки, наприклад:

a) з системами відеоспостереження, які при виникненні системної події, вже заархівованої, надсилають системі сповіщення про початок запису та повертають камеру на місце для фіксації наслідків події, позначеної як підозріла;

b) з функціями системи охоронної сигналізації (SOS) для забезпечення контролю доступу до зон обмеженого доступу або зон, налаштованих на автоматичну постановку під охорону.

Завдяки системі пожежної сигналізації (SPS) він отримує інформацію про стан від пожежних сповіщувачів, автоматичного відкриття евакуаційних дверей і закриття дверей у разі пожежної тривоги. [1, 2]

1.2 Класифікація СККД

СККД діляться на два типи – ті що у мережі та автономні.

1.2.1 Системи що знаходяться у мережі СККД

Він має атрибут, що кожен мережевий LCD пов'язаний з одним сервером на об'єкт керування доступом (контролер); тобто складається принаймні з двох частин: локальної системи автоматизації та серверної частини, яка обробляє

запити доступу від локальної системи автоматизації. Такий ССКД дуже корисний для великих об'єктів, тому що за десяток автономних дверей контролювати їх вже стає вкрай непрактично. Мережевий CCD необхідно впроваджувати в таких випадках:

Коли це неможливо або не рекомендується встановлювати повну внутрішню систему автоматизації.

Якщо систему можна розділити та скопіювати на різні частини в інших системах (наприклад, на пристрої з обмеженим доступом), тоді доведеться встановити більше апаратного забезпечення для обробки та зберігання даних, що суперечитиме підтримці та вартості системи. .

Коли немає потреби в локальних даних і продуктивність системи низька, настав час «переїхати в хмару». в особистих приміщеннях тощо.

Щоб стояти на високому рівні, система контролю доступу до мережі обов'язково повинна володіти такою здатністю розширювати та диференціювати систему контролю входу самодостатнім і легко розширюваним і керованим способом. У системах контролю доступу до мережі можуть застосовуватися бездротові технології (радіоканали). Як правило, це зумовлює використання бездротових мереж в окремих випадках, коли важко або неможливо підключити дротовий зв'язок до об'єктів, тобто збільшуються фінансові витрати при встановленні точки доступу. Варіантів радіостанцій дуже багато, але насправді деякі з них використовуються в системі ССКД.

Bluetooth. Цей протокол бездротової передачі даних зазвичай аналоговий, майже так само, як Ethernet. Його характеристика полягає в тому, що він вимагає паралельного зв'язку для підключення компонентів при роботі з протоколом RS-485. Це вирішило б недолік у цьому іншому варіанті, який погано працює з великими класами об'єктів через обмеження діапазону та деякі проблеми безпеки, доступні з технологією Wi-Fi. Це призведе до того, що це не працюватиме у великих установках, оскільки відстань до приймача (комп'ютера) буде фіксованою, і цієї проблеми необхідності підключення до

іншого користувача буде уникнуто. Це було б кращим рішенням для локальної домашньої автоматизації, яка зазвичай має лише одного користувача та зазвичай знаходиться досить близько до приймача. Але, з іншого боку, такий тип об'єднання є досить енергоефективним, тому, можливо, це корисно в ситуаціях, коли система переходить у режим очікування, щоб виробляти електроенергію.

Wi-Fi. Однією з істотних переваг цієї радіочастоти є міжміський зв'язок, який може покривати кілька сотень метрів. Це особливо важливо для з'єднання віддалених об'єктів. Таким чином, економляться час і фінансові ресурси на прокладання комунікацій. Крім того, цей вид зв'язку забезпечує додатковий рівень безпеки, пов'язаний з пакетами в потоці. Якщо такий вид з'єднання добре зібраний, можемо бути впевнені, що робота буде завершена належним чином, оскільки воно передає пакети як серверу, так і користувачеві. м

1.2.2 Системи що не знаходяться у мережі СККД

Автономні системи набагато дешевші в експлуатації, жодним чином не потребують прокладання кількох сотень метрів кабелю, додаткових пристроїв, які підключаються до сервера, або навіть самого сервера. Зворотно пов'язані зі сказаним вище такі негативні сторони такого типу системи, як нездатність генерувати звіти, відсутність інформації про час її безвідмовної роботи, відсутність контролю подій і навіть відсутність можливості дистанційного керування нею. Кілька типів цієї системи були описані вище. Насправді один із найбільших ризиків полягає в тому, що ви не збережете пароль, про який згадувалося вище. Крім того, такий тип системи має значні обмеження щодо застосування. Проте навіть із системою цього типу, як пояснювалося вище, окрім здатності продовжувати працювати, коли один критичний компонент не працює, система є стійкою до збоїв щодо втрати зв'язку із сервером, подібно до мережі. Він радше розміщуватиме ССД, які виникатимуть, як тільки член класу

втрачатиме зв'язок із сервером. Тип ПЗЗ у цій категорії не є найбільшою проблемою, оскільки інші системи не можуть працювати також. При виборі автономної системи з високими вимогами безпеки враховуйте наступне:

- Зчитувач повинен бути ізольований від контролера, щоб не було зовнішніх проводів до зчитувача, які могли б відкрити замок.
- Контролер повинен мати альтернативне джерело живлення, якщо це зазвичай є безвідмовною вимогою.

Система самостійного доступу також використовує електронні замки, які передають дані через бездротові канали: двері мають механічний замок з електронним керуванням і вбудованим зчитувачем. Замок спілкується з концентратором через радіочастотний канал, який, у свою чергу, спілкується дротом з робочою станцією, де встановлено програмне забезпечення.

1.3. Сучасний стан систем СККД

З кожним роком кількість людей, стурбованих технологіями ідентифікації обличчя, зростає, і сьогодні вже кілька десятків систем впроваджено в різні сфери людської діяльності.

Лідерами ринку в цьому напрямку є такі компанії, як NEC Corporation (Японія), Cognitec Systems GmbH (Німеччина), Neurotechnology (Литва).

Система FaceVACS-ВідеоСкан

Він простий у використанні, оскільки він регулюється та представляє програмне забезпечення для розпізнавання обличчя в реальному часі від Cognitec Systems. Роботу системи «FaceVACS-Video» забезпечує її компонент, який називається FaceVACS-VideoScan:

- сервер потокового відео; керує відеопотоком;

- сервер відеоспостереження координує всі компоненти системи та виконує основні біологічні операції;

- обчислювальний вузол, призначений для розрахунку розподілу обчислювальних навантажень.

Інтерфейс користувача:

- Менеджер сигналів, який отримує сповіщення про події та керує мобільними пристроями, оперативною базою даних та набором інтеграторів.

До теперішнього часу технологія FaceVACS розгорнула алгоритм B10T9 для розпізнавання обличчя. Він був стійкий до міміки, повороту обличчя ($\pm 15^\circ$), часткового закриття ока, носіння захисних окулярів та зміни освітлення. Крім того, FaceVACS наділений такими функціями:

- багатоцільове відстеження;
- повторна ідентифікація суб'єктів у режимі реального часу;
- відображення та передача статистичних даних про потоки;
- інтерактивна реєстрація власності;
- C++ API та API веб-служб

Система розпізнавання обличчя NEC

Це одна з найдосконаліших систем розпізнавання обличчя в японській країні, розроблена компанією NEC. Ця система може розпізнавати людей із фільмів десятирічної давнини, навіть якщо вони носять окуляри, і це зовсім нестандартно. Усі розпізнані обличчя зберігаються в базі даних: якщо вам потрібно отримати доступ до всієї історії реєстрації відео, просто відкрийте реєстраційну інформацію та дату й час будь-якого раніше збереженого зображення.

Ця технологія перевершує поточні системи розпізнавання — як за швидкістю, так і за точністю. Він працює з низькоякісним відео, сильно стиснутими зображеннями та багато іншого. NEC оцінює особисті характеристики людини (розмір, форму зіниць, лінії носа та рота та їхнє

просторове відношення до інших осіб у своїй базі даних), а потім порівнює іншу особу у своїй базі даних на основі цієї інформації. [3-8]

Система містить різні модулі, які реалізують наступні алгоритми:

1. Узагальнений метод переслідування (GMFD) має високу швидкість виявлення та високу точність розпізнавання облич. GMFD базується на нейронних мережах, які спочатку шукають пари очей.

2. Алгоритм PSM допомагає вирішити задачу з'ясувати, де в кадрі стоїть людина (хтось під кутом або просто за межами кадру).

Метод ARBM (Adaptive Regional Blend Matching) зменшує вплив незначних змін обличчя на точність розпізнавання (наприклад, вираз обличчя, окуляри, головні убори). Нижче наведено особливості системи розпізнавання обличчя NeoFace:

- можливість моніторингу та налаштування в реальному часі;
- ідентифікація фізичної особи;
- кілька підтверджень;
- пошук подій в базі даних;
- журнал записаних зображень осіб;
- гнучкість для нових напрямків руху до 45 градусів від поточної позиції;
- елемент управління «перетягування»;
- великий розмір і необмежену ємність бази даних;
- незалежно від напрямку очей або характеристик обличчя (окуляри, борода) або виразу обличчя.

Для системи Neurotechnology VeriLook SDK

VeriLook SDK — це продукт компанії Neurotechnology, який реалізує систему ідентифікації людини. Ця система розпізнає людей по обличчю, а потім визначає їх у короткий термін (до 100 000 облич за секунду). VeriLook SDK пропонується як цілий комплект розробки програмного забезпечення для великої кількості пристроїв, що працюють під керуванням Windows, Linux, Mac

OS X, iOS та Android. Алгоритм VeriLook застосовує технологію глибокої нейронної мережі в обробці цифрових зображень для локалізації людини.

Немає взаємодії з пристроями сканування обличчя. Швидке впровадження клієнтських додатків для біометричної ідентифікації особи. Інші плюси:

- обробка кількох осіб одночасно.
- оцінка статі. крім того, для кожної людини на портреті також можна позначити підлогу.

- розпізнавання обличчя в реальному часі. VeriLook перевірить, чи людина на відео жива, чи це зображення;

- розпізнавання емоцій. VeriLook розглядає шість основних емоцій: гнів, огиду, страх, щастя, смуток і здивування. Інтерфейс особистих характеристик. Під час налаштування зйомки обличчя VeriLook може зв'язати будь-який із двох результатів під час зйомки зображення: наприклад, із посмішкою чи без неї;

- визначення привабливості зовнішнього вигляду обличчя. Під час реєстрації ідентифікаційних даних може бути встановлений поріг якості, щоб у базі даних зберігалися лише найкращі шаблони.

Окремі екземпляри однієї особи. Такі зразки можна переглядати різними способами та в різний час; таким чином якість порівняння покращується.

Доступ до. Параметри VeriLook доступні як для 1-до-1, так і для кількох режимів порівняння ((ідентифікація));

Дизайн шаблону обличчя. Шаблон особи може мати розмір 4 байти;

Загальний режим плюс бали. Наявність встановленого діапазону атрибутів обличчя на рівні зображення для самого зображення;

Алгоритм VeriLook розпізнає ці межі, що спостерігаються в інфрачервоному спектрі.

1.4 Аналіз систем СККД як об'єкту автоматизованого керування

Основні елементи СККД.

1.4.1 Пристрої загорожі

Вони дуже різноманітні, наприклад, турнікети, двері з електромагнітним ключем тощо.

Більшість із них, коли подається живлення, вимикаються, тому їх популярно використовувати на шляхах пожежної евакуації.

Турнікети - механізм перемикання від поворотного до розсувного за допомогою певних штирів, що обмежують його рух. Він не повинен зупинятися, а лише обмежувати швидкість, щоб полегшити проїзд у будь-якому випадку. Якщо ще потрібна перевірка користувачів.

Електромеханічні замки – вони досить стійкі до злому (якщо замок механічно справний), а також мають механічний скидання (якщо натиснути на замок, він буде розблоковано, поки ви не відчините двері). [8-12]

Кабіни-шлюзи: працюють у банках, у режимних установах.

Ворота та шлагбауми в основному розташовуються на території підприємства, на стоянках автомобілів та за автостоянками, на в'їздах комерційних будівель, у дворах житлових будинків. Основна вимога — можливість експлуатації в кліматичних умовах і можливість автоматизації (для систем контролю доступу). Існують додаткові вимоги до конструкції організації контролю доступу до системи — розширена функція включає можливість зчитування номерних знаків (розмір більше терміну використання, застарілий), можливість розпізнавання номерів автомобілів (у разі застосування з відеоспостереження).

1.4.2. Засоби ідентифікації

Випускається в найбільш звичайних варіантах виконання: картка, брелок, наклейка і т. д. Це найбільш поширені типи зчитувачів. Система в основному є ключовою функцією для роботи будь-якої системи контролю доступу, яка формує права власника відповідно до використовуваних кодів («ідентифікація»). Це може бути сенсорна карта пам'яті, безконтактна картка RFID-смарт-карта або карта з магнітною смугою. Ключ дозволяє налаштувати функцію програми та запустити цю функцію. Це буде з біометричними зчитувачами, порівняно з деякими з яких є: відбитки пальців, візерунок райдужної оболонки ока, 3D-фотографія людини, капілярний малюнок містить кров під шкірою долоні.

Надійність (стійкість до підробок) системи контролю доступу залежить від рівня використовуваного ідентифікатора. Більшість безконтактних карток легко підробити на обладнанні, яке дуже легко ідентифікувати; отже, такі ідентифікатори навряд чи будуть застосовані до елементів, які вимагатимуть більшого захисту. Набагато більша різниця в безпеці з RFID, які застосовують набагато вищий рівень безпеки, оскільки код картки зберігається в захищеній зоні та закодований. Це теж небезпечно, оскільки не потрібно розкодувати тег, а його кодоване значення можна відтворити на іншому пристрої. Нарешті, існує набагато більш точний метод, як вже згадані біометричні дані. Не всі біометричні дані представлені у вигляді звичайного тексту; отже, вам потрібно використовувати такий, який можна зчитувати без додаткового обладнання, окрім камери чи іншого пристрою, щоб отримати інформацію за короткий час. Він має ці атрибути сітківки, підписом яких є обличчя на фотографії. Але тоді виникає проблема збереження даних, оскільки це особиста інформація, за винятком обличчя, і може використовуватися в іншій системі. У наш час навіть на мобільних телефонах є зчитувач відбитків пальців, ця інформація важлива, тому не варто її підробляти. На відміну від обличчя, дані дуже важко підробити

за допомогою картки 3D-тегів, оскільки для цього знадобиться таке обладнання, а за допомогою лише фотокартки неможливо буде отримати доступ до системи без обличчя. Крім того, зчитувач у системі працює за тією самою технологією, тож із простою фотокарткою доступ знову буде заборонено без обличчя. [10-17]

1.4.3 Засоби контролю

Він є невід'ємною частиною системи: визначає особу, яка має право проходити через точку доступу, зберігає коди в списку прав доступу ID, визначає права власника. Коли людина зчитує (подає читачеві) код, з ним проводиться порівняння і на основі цього приймається рішення. Він працює з певною потужністю. Таким чином, контролери забезпечуються окремою батареєю більшу частину часу, яка підтримує його роботу протягом кількох годин або днів у разі збою живлення. Однак у дуже складних системах контролер частіше бере участь у процесі керування без фактичної обробки даних. Він приймає рішення на основі результатів, які сервери можуть отримати після обробки певного набору даних. Контролер є основним елементом локальної системи автоматизації та обробляє сигнали датчиків. Він передає команди виконавчим механізмам.

1.4.4 Засоби зчитування

Це пристрій, який отримує ідентифікаційний код. Існують різні варіанти зчитувача залежно від ідентифікатора. Для «таблетки» складається з двох електричних частин, одна з яких називається «кишенькою». Для карти, яка складається з друкованої плати та антени, у цьому прикладі зображення має містити телекамеру. Якщо зчитувач буде встановлений на шляху (ворота, вхідні двері будинку, в'їзд на паркінг), то необхідно, щоб пристрій витримував

кліматичні навантаження, такі як перепади температури, опади, а особливо якщо регіон є несприятливим кліматом, то він повинен мати здатність йому протистояти. Якщо існує небезпека вандалізму, слід також враховувати механічну міцність (сталевий корпус). Окремо вибираються зчитувальні пристрої для ідентифікації об'єктів на відстані до 50 м. Це корисно на високих і автомагістралях, а також на блокпостах. Користувачі, які підписалися на теги — як правило, мають активні теги (містять інтегровану батарею) — оголошуються. Ультразвукові датчики створюють зображення (відбиток), яке не відповідає стандартній техніці авторизації відбитків рук або пальців. Ультразвукові датчики створюють зображення в приміщеннях, де існує політика конкретності та точності зображення; тому їм неможливо обійтися без ультразвукових датчиків. Буде потрібна камера глибини як засіб перевірки у випадках, коли використовується обличчя.

1.5. Постановка задачі досліджень

Після детального аналізу існуючих рішень і підходів були визначені вимоги, які б відповідали вищезазначеним умовам. Щоб система була застосована, мають бути виконані наступні передумови:

- можливість зв'язку з усіма периферійними пристроями через одну універсальну точку доступу;
- швидкість системи;
- здатність до збільшення;
- можливість зберігати та додавати інформацію про нових та старих користувачів;
- можливість редизайну системи без її зупинки;
- масштаб системи як у вертикальному, так і в горизонтальному напрямках;
- стійкість системи.

Після того, як всі вимоги були виконані, мали можливість спостерігати всю проблему та вибирати підходи до її вирішення.

1.6 Висновки до першого розділу

Таким чином, можна зробити висновок, що система контролю та управління доступом не є нещодавньою розробкою, але вже досягнута в цьому напрямку, але все ще не має остаточного вирішення проблеми захисту швидкості з точки зору контролю доступу. Оскільки швидкість у напрямку схилу висока, входять у вжиток картки або мітки, які можна підробити. Зі збільшенням глибини захисту починають помічати деякі проблеми з налаштуваннями системи та особисті дані починають втрачатися. РК-телевізори сьогодні не забезпечують розпізнавання обличчя, навіть якщо вони виконують завдання доступу та безпеки.

2 РОЗРОБКА МОДЕЛІ АВТОМАТИЗАЦІЇ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ

Система контролю доступу (СККД) – це складна система, яка складається з значної кількості компонентів, як апаратних так і програмних.

2.1 Опис характеристик керування

Рух документується як частина системи контролю та управління доступом за допомогою дискретного датчика руху; фото зображення. Після того, як контролер обробляє фотографію через модель, керуючим впливом є сигнал, створений контролером, який, у свою чергу, передається на вихід у вигляді двійкового числа. У зазначеному прикладі живлення є, але не надсилається на плату керування приводом. [12-19]

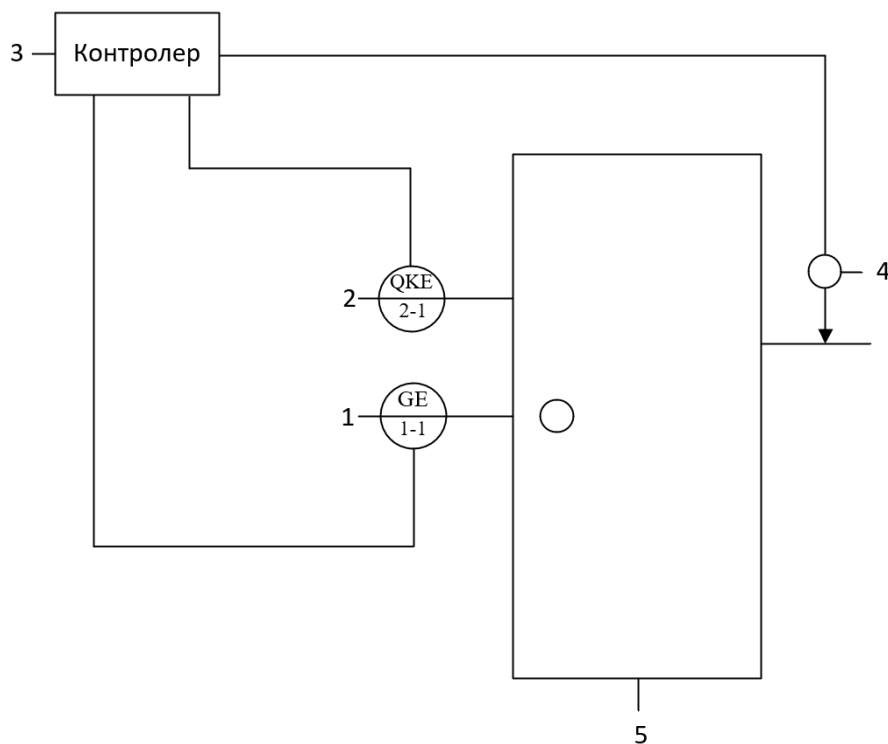


Рисунок 2.1 - Функціональна схема управління СККД

П'ять основних системних елементів, зображених на функціональній схемі СККД (рис. 2.1.), є такими:

1. Датчик руху (інфрачервоний випромінювач і приймач).
2. Камера для документування зображень.
3. Контролер для взаємодії з системою.
4. Механізм закриття.
5. Пристрій блокування фізичного доступу.

Він працює за такими принципами: людина, яка хоче увійти в кімнату, наближається до існуючого фізичного бар'єру. Потім спрацьовує датчик руху, який посилає сигнал на контролер. Потім цей сигнал розшифровується контролером, який дасть камері команду зробити знімок. Після того, як він робить знімок, він надсилає його до контролера, який обробив його за допомогою моделі. Отримавши результат (% подібності), контролер вирішить, надати чи заборонити доступ, надіславши їм сигнал (зазвичай виконавець зазвичай закритий).

2.2 Обрання платформи для створення локальної системи автоматизації

Вибір типу контролера - перший крок у створенні будь-якої системи. Щоб можна було вважати цю проблему вирішеною, зупинимося на одній з найбільш поширених платформ для невеликих завдань локальної автоматизації — Arduino або Raspberry Pi. Отже, обговоримо кожен докладніше.

Arduino — це компактне обладнання, яке містить процесор ATmega та пам'ять. Плата має 6-12 аналогових виходів, а також 12-24 цифрових виходу залежно від моделі. Він може безпосередньо взаємодіяти з різними датчиками або механізмами керування, за винятком попередньої обробки чи стандартизації сигналу. Аналогові датчики мають цифрові контакти, і навпаки. Загальна схема плати Arduino показана на малюнку 2.2. Недоліком, який можна

приписати цій платформі, є її послідовний характер, оскільки платформа здебільшого синхронізована, тобто не підтримує кілька операцій одночасно.

Переваги рішення:

- малі габарити;
- прототип можна зробити швидко;
- низьке енергоспоживання;
- відсутність обов'язкового охолодження.

Недоліки:

- неможливо безпосередньо підключити зовнішні пристрої. сьогодні багато таких жорстко вимагають виділеної шини введення-виведення даних;
- відсутність асинхронності або паралелізму; тому операції не можна виконувати окремо одна від одної;
- немає вбудованого рішення для підключення до мережі.

Це рішення сумісне з дизайном і використанням у невеликих об'єктах, у яких може бути висока видимість основної частини; однак таке налаштування не типово. Як і у випадку з основним рішенням, підключення пристроїв вводу/виводу безпосередньо до контактів і їх паралельна обробка є неможливим. Швидше за все, це перешкоджає використанню цього рішення без певних окремих проміжних компонентів, які, у свою чергу, стають вразливими до системних збоїв, вводячи більше елементів у ланцюг.

Raspberry Pi – це скоріше повноцінний одноплатний комп'ютер, на відміну від мікроконтролера Arduino. Враховуючи той факт, що процесори ARM побудовані на платформі Raspberry Pi, тому ця платформа є більш гнучкою. Аналоговий і цифровий зв'язок підтримується Raspberry Pi. Крім того, ця система має багато інформаційних шин вводу/виводу, які можна підключати до інших датчиків, камер і системних периферійних пристроїв. Крім того, на відміну від Arduino, це рішення може працювати як в асинхронному, так і в багатопоточному режимі, що дозволить нам паралельно обробляти інформацію

та виконувати дії, такі як введення з камери та посилання на актуатор, набагато швидше.

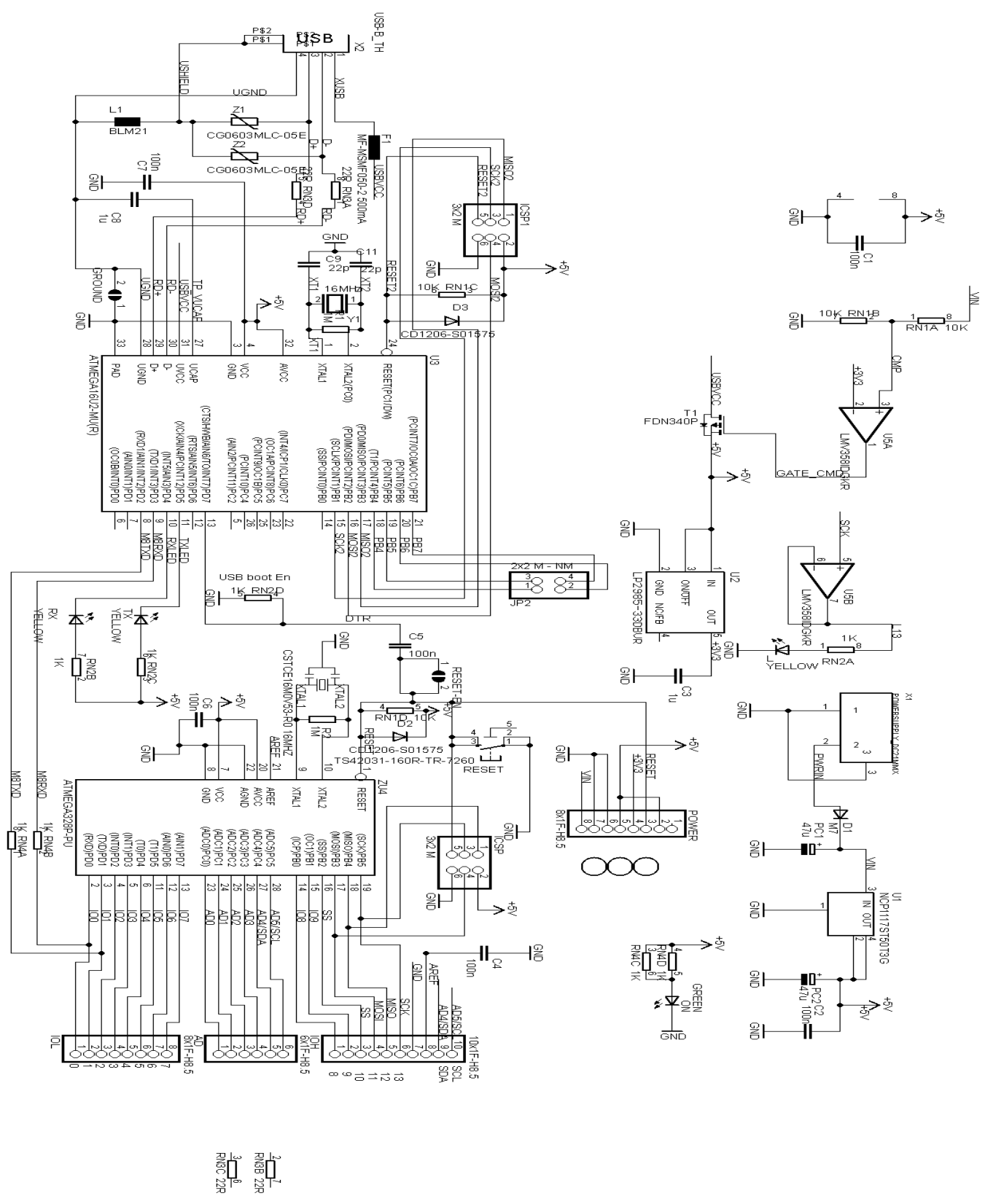


Рисунок 2.2 – Принципова схема модуля Arduino

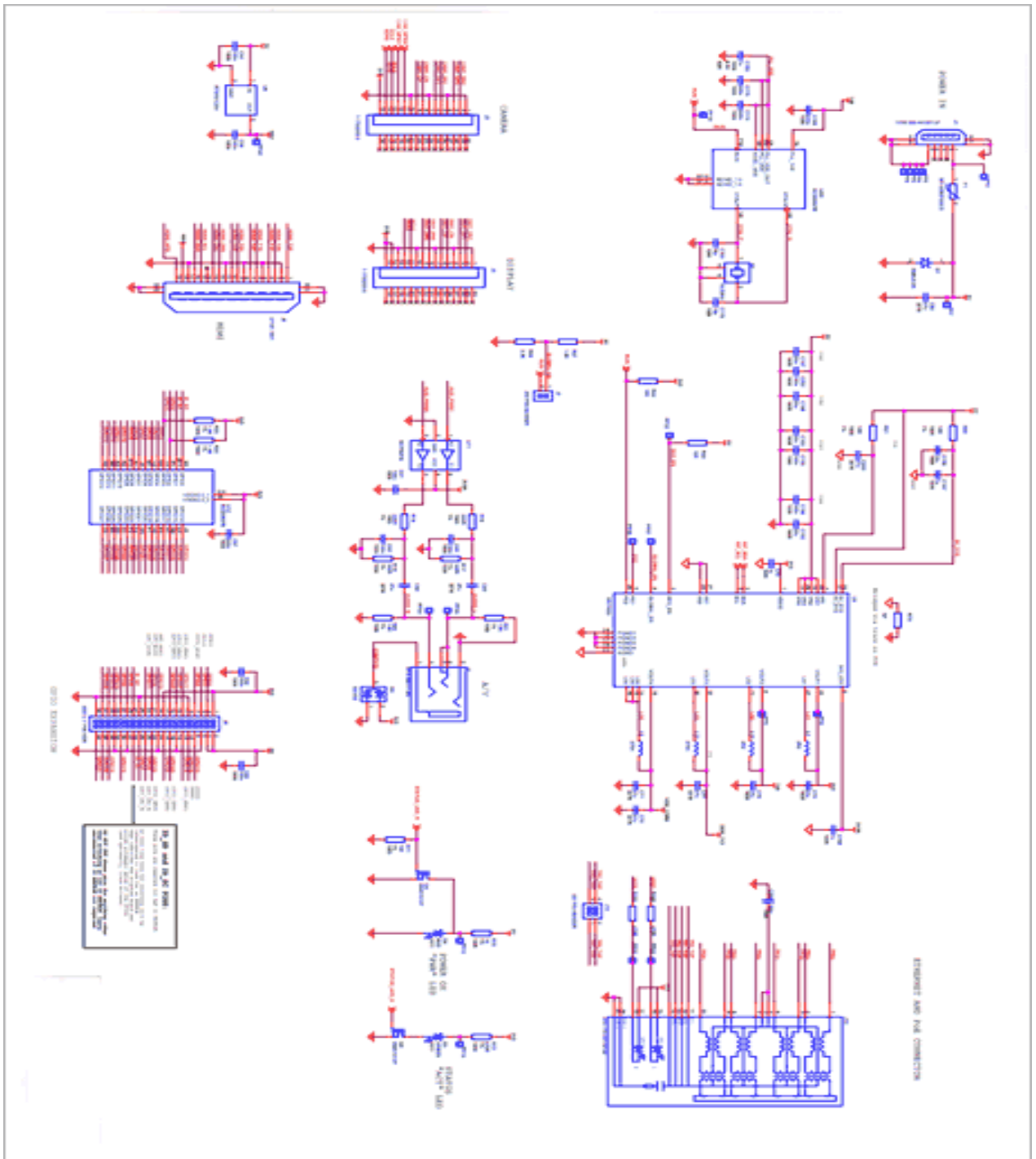


Рисунок 2.3 – Принципова схема Raspberry Pi

Це однозначно допоможе збільшити швидкість обробки інформації за рахунок паралелізму потоку даних. На рисунку 2.3 зображено принципову схему цього комп'ютера. [18-25]

Переваги цього рішення:

- усі типи периферійних пристроїв (камери, детектори руху, приводи тощо) можуть бути підключені безпосередньо до них;
- пристрої як бездротові, так і дротові.

Негативні сторони цього рішення:

- споживання електроенергії досить велике;
- охолодження – це те, з чим доведеться боротися.

2.3. Проектування застосунку

Сьогодні використовується багато шаблонів архітектури програмного забезпечення. Давайте розглянемо три, які можуть допомогти вирішити поставлену проблему:

- «моноліт».
- дизайн «малі послуги».
- клієнт-серверний дизайн.

Монолітна архітектура. Монолітна архітектура фактично являє собою традиційний дизайн програмного забезпечення, в якому розробляється окремий модуль для подальшого запуску програми. Моноліт часто описують як великий і некерований, два слова, які добре описують загальну архітектуру розробки програмного забезпечення.

Це велика єдина мережа з єдиною кодовою базою для об'єднання всіх бізнес-завдань. Оновлення в цій програмі означає, що вам доведеться спочатку оновити весь стек через кодову базу, а потім випустити оновлену версію сервіс-орієнтованого інтерфейсу та розгорнути її. У результаті оновлення стає неможливим і займає дуже багато часу.

Моноліти зручно використовувати на ранніх стадіях проектів для розгортання коду без особливих розумових зусиль щодо обслуговування. Це дає змогу негайно випустити все в програмі як монолітну на рис. 2.4: ілюстрована схема монолітного дизайну. Це в основному відображає всі складові елементи, упаковані в одну програму. Все це виконується через єдиний механізм, розташований в одному місці як єдиний сервіс. [26-32]

Переваги конструкції

- легкий монтаж: використання одного виконаного файлу або каталогу полегшує розгортання;
- розвиток: оскільки програма розроблятиметься на основі єдиного коду, розробка програми стає легкою;
- продуктивність: в єдиному репозиторії та центральній кодовій базі один єдиний API можна прийняти як інтерфейс для кількох/кількох мікросервісів раз і назавжди.

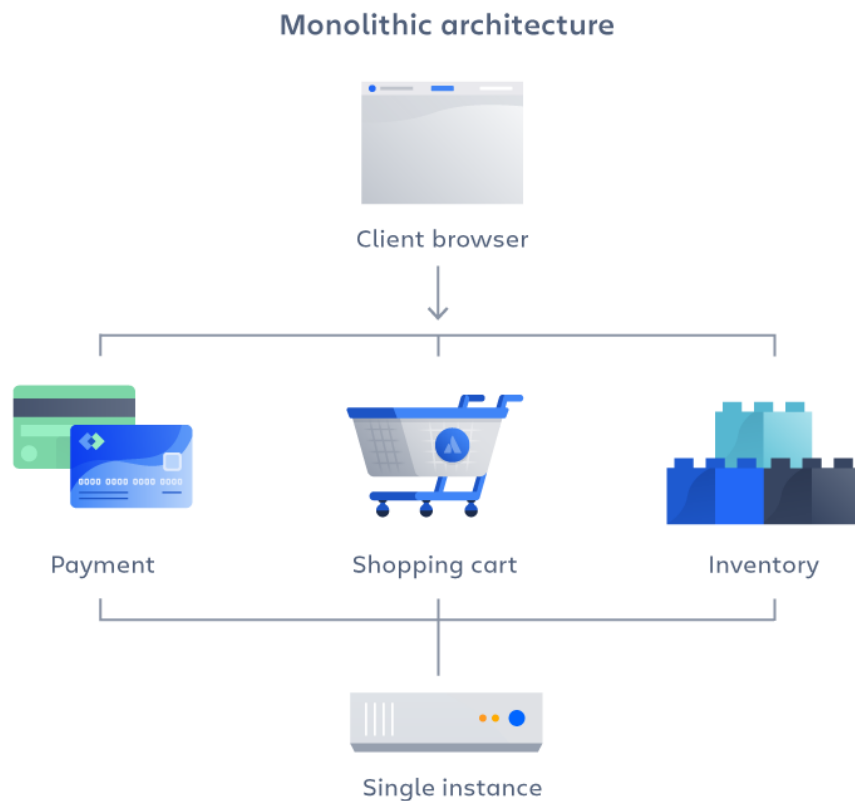


Рисунок 2.4 Схематичне виконання монолітної архітектури

- скорочене тестування: додаток monolith є єдиним централізованим блоком, тому тестування всієї системи відбувається набагато швидше, ніж для розподіленого додатка.

- легке усунення несправностей: весь код в одному місці; отже, ви можете легко виконувати запити, щоб знайти будь-яку проблему, яка може виникнути.

Недоліки цієї конструкції:

- низька швидкість росту. Одна велика міцна програма створюється дуже повільно, і розвиток лише однієї є маленькою частиною;

- масштабованість. Неможливо змінити окремі компоненти;

- міцність. Якщо одна частина виходить з ладу, це знижує доступність програми;

- не гнучкий. Технологія, інтегрована в програми, обмежена тим, що вона може робити;

- проблеми впровадження тех. Усе, що стосується змін в інфраструктурі чи мовах програмування, автоматично тягне за собою внесення змін у всю програму, що зазвичай вимагає додаткових витрат і часу;

- реалізація. Незначні зміни потребуватимуть перетворення всієї монолітної програми.

Наступний рівень архітектурної абстракції відомий, розглядаючи «мікросервіси». Архітектура мікросервісів (або просто «мікросервіси») — це нова/стара дитина на блоці сервіс-орієнтованої архітектури, де все працює незалежно як самодостатня служба; тобто кожна служба має власну логіку та відповідну базу даних для задоволення цієї конкретної потреби. Тестування розгортання та масштабування є внутрішніми для кожної служби. Мікросервіси розбивають великі бізнес-завдання на багато окремих кодових баз. Це не означає, що мікросервіси зменшують складність; скоріше вони приховують складність на потрібному рівні, розділяючи роботу на окремі одиниці виконання та взаємодії на більших масштабах сприйняття. Склад компонентів цієї архітектури показаний на рисунку 2.5.

Нижче наведемо наступну архітектурну парадигму – «мікросервіси». Архітектура мікросервісів (або просто «мікросервіси») — це архітектурний стиль, який структурує програму як набір слабо пов’язаних служб, які, у свою чергу, мають бути незалежно розгорнуті та масштабовані (як у випадку з службами, де навіть тестування може бути розглядається як внутрішня функція). Мікросервіси розбивають великі бізнес-завдання на безліч менших окремих кодових баз. Мікросервіси можуть не зменшити притаманну складність, але вони роблять її явною та контрольованою, розбиваючи дії на підпроцеси, які є автономними по відношенню один до одного та сприяють більшому благу.

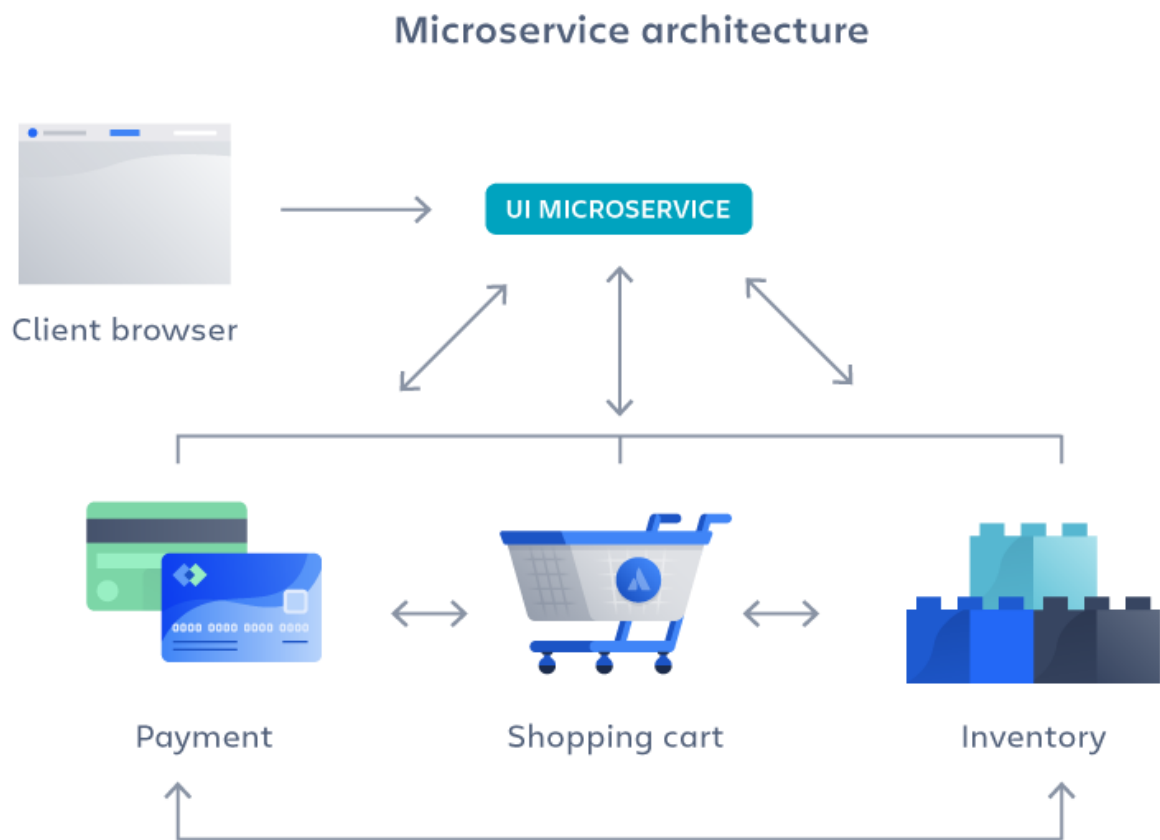


Рисунок 2.5 – Схема структурна “Мікросервісної” архітектури

Переваги:

- простота обслуговування та тестування. Команди можуть легко зрозуміти нову функцію та повернутися до попередньої версії, якщо потрібно. Це зменшує труднощі оновлення кодів і швидко відстежує відкритість нових функцій для громадськості. Крім того, в окремих сервісах легко знайти помилки та проблеми;

- розгортання незалежного хостингу. Оскільки мікросервіси розглядаються як окремі компоненти, можна легко та швидко реалізувати окреме розгортання окремих функцій;

- технологічна гнучкість. Завдяки дизайну мікросервісів більшість команд можуть вибрати інструменти, які їм найкраще підходять;

- 100% надійність. Незалежно від того, які зміни ви застосовуєте до служби, збій програмного забезпечення не викликає страху.

Причини такого вибору такі:

- розвиток зростання складніше. Серед усіх інших проектів у світі мікросервіси ускладнюють монолітну архітектуру просто тому, що існує більше сервісів, які, швидше за все, створені різними командами в різних частинах світу. Якщо ріст не регулюється належним чином, це сповільнить розвиток з точки зору продуктивності;

- збільшення вартості інфраструктури. Для кожного нового мікросервісу є пов'язані витрати з набором тестів, інструкціями з розгортання програмного забезпечення, інфраструктурою розміщення програмного забезпечення, інструментами моніторингу програмного забезпечення тощо;

- інші витрати на організацію. Командам знадобиться більше спілкування та співпраці, щоб швидко звільнити місце для оновлень і взаємодії;

- налагодження. Проблеми в журналах кожного мікросервісу ускладнюють процес налагодження. Додаткові ускладнення також можуть виникнути, якщо один бізнес-процес має працювати на кількох машинах;

- все не стандартизовано. Відсутність спільної платформи може призвести до збільшення списку мов, стандартів журналювання та інструментів моніторингу.

Переходимо до наступної в списку архітектур — «Клієнт-сервер». "Клієнт-сервер" дуже простий, якщо розбити на два різні рівні.

- клієнт: клієнт — це локальний комп'ютер або будь-який інший пристрій, увімкнений для обчислень, який функціонує як віртуальний користувач і зазвичай запитує дані або конкретну групу дій, які повинні виконуватися сервером (або від його імені);

- сервер: сервер — це потужний комп'ютер або спеціальне системне обладнання, призначене для виконання програм із вищою швидкістю. Він виконує певну роботу від імені своїх клієнтів, надає користувачам доступ до певних ресурсів системи, зберігає дані або обробляє запити з бази даних.

Атрибути моделі вимагають, щоб користувач вказав дію, яку має виконати сервер, після чого дія автоматично обробляється, а результат передається клієнту. Сервер може обробляти багато клієнтів послідовно.

Якщо одночасно надходить більше ніж 1 запит, запити розміщуються окремо, і сервер оброблятиме їх у тому порядку, в якому вони були розміщені. Іноді запити встановлюють певні пріоритети. Тим не менш, навіть найкритичніші завжди будуть обслуговуватися в порядку живої черги.

Параметри, реалізовані на сервері:

- зберігання, захист і доступ до даних;
- робота за запитами клієнтів;
- повернення роботи замовнику.

Параметри під контролем клієнта:

- ініціює та взаємодіє з графічним інтерфейсом користувача;
- викликає сервер для виконання дії, а потім повертає результати дії.

Після отримання результатів запиту видає додаткові команди < додати/оновити інформацію або видалити групу даних >.

Така система дає можливість брати участь у кількох ідентичних проектах, що в зазначеному випадку забезпечить поширення системи та її подальше використання в різних компаніях. Крім того, при об'єднанні з попередньо створеною базою даних це полегшує налаштування різних частин системи без зміни коду програми, змінюючи лише базу даних.

У результаті вищевикладеного можемо сказати, що для запропонованої системи автоматизації найбільш підходящим підходом до розробки програмного забезпечення — з огляду на швидкість, конфігурацію та простоту створення та обслуговування є «архітектура клієнт-сервер».

Вибравши клієнт-серверний дизайн додатків, матимемо міні-комп'ютер, який діятиме як клієнт, тоді як сервер буде розроблено на мові програмування Python і виконуватиме роль передачі даних між базою даних, нейронною мережею та клієнтом. [26-32]

Схема складається з чотирьох основних блоків.

- Raspberry Pi – пов'язаний із клієнтським компонентом;
- сторона сервера;
- модель машинного навчання (модель ML) — для розпізнавання та навчання разом із попередньою обробкою даних;
- периферійний блок - зовнішні компоненти.

Якщо компоненти та периферійні пристрої присутні у фізичній формі, яка знаходиться безпосередньо в установці, інші компоненти є програмними додатками, розташованими на сервері або в «хмарі». Raspberry Pi та його периферія спілкуватимуться один з одним через паралельну шину даних у синхронному режимі. Це означає, що до тих пір, поки він не отримає сигнал від датчика руху, периферійний блок залишатиметься нерухомим.

Ця взаємодія здійснюється шляхом виконання «Сервера», «Моделі машинного навчання» та «Raspberry Pi» через Rest API, що є підходом, заснованим на використанні запитів HTTP.

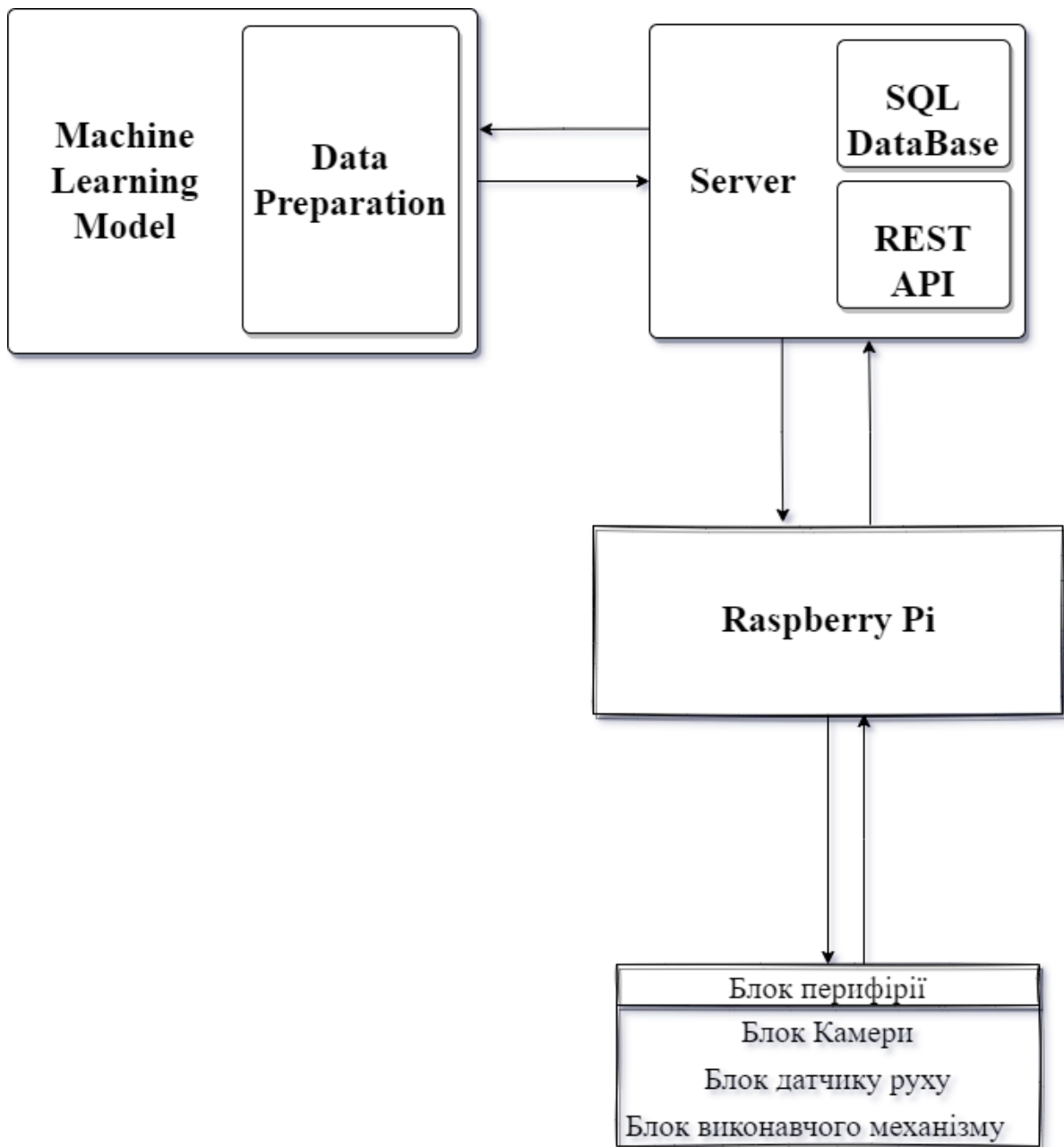


Рисунок 2.6 - Структура архітектури застосунку

2.4 Обрання бази даних

Сучасні бази даних можуть бути розроблені відповідно до двох різних типів: OLAP і OLTP. OLAP — це онлайн система керування базами даних аналітичної обробки, призначена для обробки аналітичної інформації майже в реальному часі. Оскільки аналітика, як правило, є величезними даними, їх

спочатку слід спеціально обробити, і, отже, ці дані спеціально розроблені для цілей статистики та показників, що означає, що вони дозволяють зберігати проміжні результати обчислень. Ця специфіка призводить до того, що основною одиницею роботи в базі даних OLAP є стовпець, оскільки в більшості випадків цікавлять дані, які описують певний атрибут об'єкта в різний час.

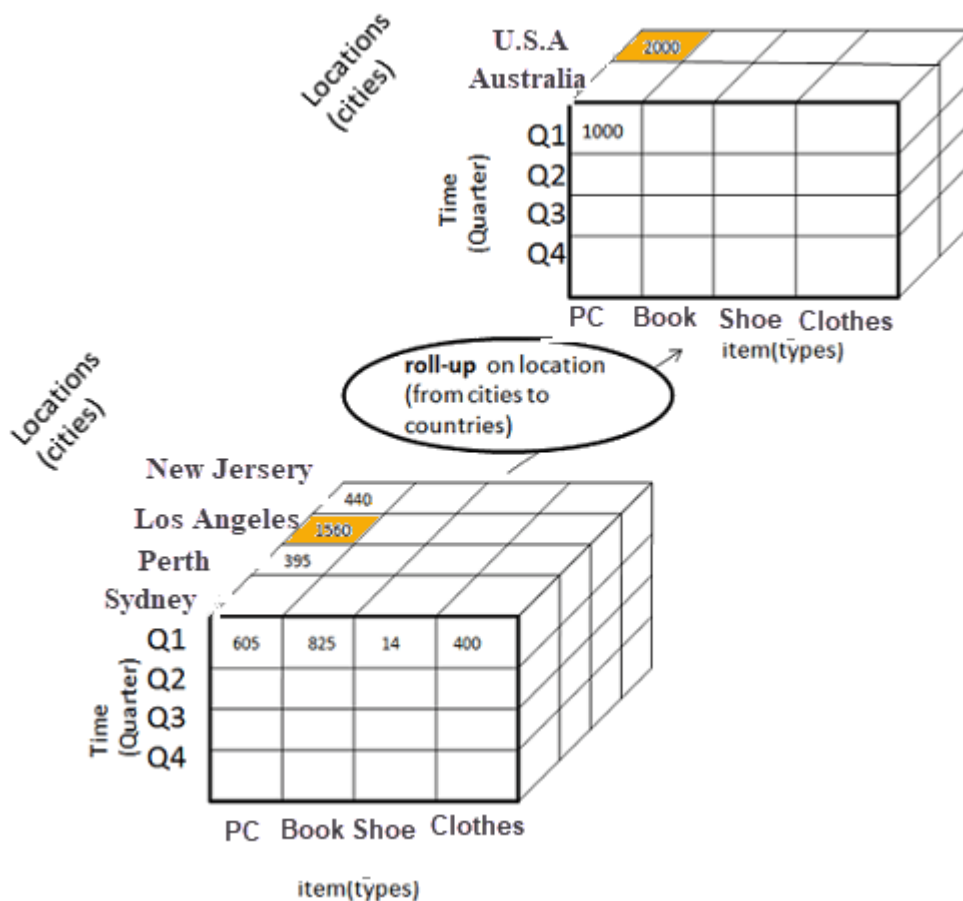


Рисунок 2.7 - Зображення схематичне OLAP у вигляді кубів

Це тип бази даних, яка використовується для OLTP (онлайн-обробка транзакцій), яка працює на основі надсилання транзакцій (пакетів запитів, що містять певні дані) з низькою затримкою та великим обсягом. Це підходить для використання в базах даних, у яких дані змінюються невеликими обсягами зі

статистичною обробкою, яка не є спеціальною на рівні бази даних. Ці бази даних також продуктивні для збереження даних, які не змінюються.

Основні відмінності виникають залежно від способу обробки отриманої інформації. Для OLAP стовпець використовується для всіх арифметичних і статистичних обчислень, що дозволяє легко виконувати обчислення над величезними даними без явного представлення, як у випадку баз даних, що працюють на OLTP. Тим не менш, база даних OLAP створена не для частого оновлення; він не підтримує цілісність даних, і, якщо під час роботи сервера бази даних трапляються неправильні дані, він повертається з того стану, який був на момент обробки цього конкретного запиту. OLTP розрахований на дедлайни і невеликі, але досить часті запити на обробку вхідних даних. Не менш важливо, якщо база даних не може вставити або оновити дані, вона буде повернена до початку транзакції (обробка даних). [33-40]

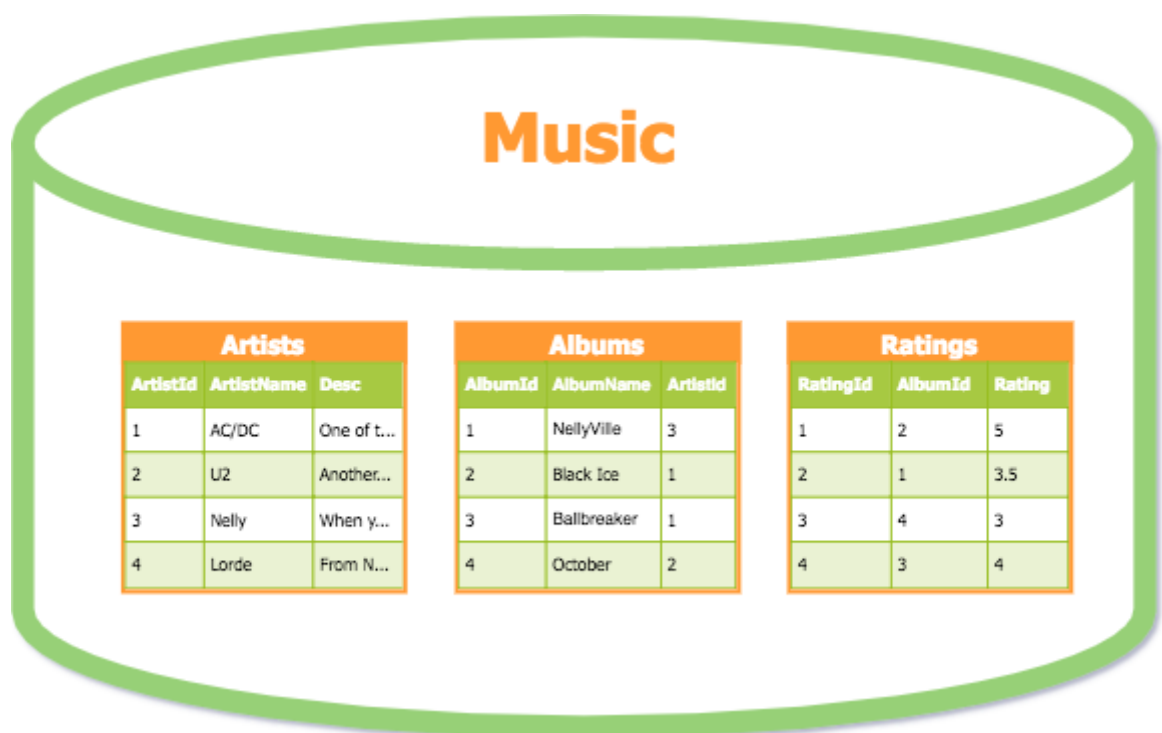


Рисунок 2.8 - Зображення схематичне OLTP у вигляді таблиці

Розглянувши деталі цих двох типів баз даних і порівнявши їх із поставленими вимогами, зазначимо, що було обрано дизайн організації бази даних типу OLTP.

Після того, як вибрали тип організації бази даних, виникає інше питання, який тип баз даних використовувати — їх можна розділити на дві основні категорії: реляційні та нереляційні.

Реляційні бази даних зберігають структуровані дані; наприклад, інформація про пристрої, датчики та людей. В основі дизайну бази даних лежить структурування організації. Бази даних без зв'язків справляються з цим зовсім інакше; Використовуючи документно-орієнтовані бази даних як приклад, інформація була збережена в деревоподібній структурі, тоді як, загалом, дані зберігаються як набір значень атрибутів з більш ніж одним, на відміну від реляційних баз даних, які можна розділити на багато таблиці. Деякі з колишніх баз даних включають PostgreSQL, MS SQL або Oracle DB, серед інших. Останній — MongoDB, Cassandra або Redis. [33-40]

Для SKD дані впорядковуються та відомі перед поверненням до системи. Отже, тип реляційних баз даних, які були обрані, відомий як PostgreSQL.

2.5 Монтажно-комутаційна схема автоматизації СККД

Рис. 2.9 ілюструє склад і спосіб комутації підключення системи автоматизації доступу, склад і комутацію технологічного процесу.

На цьому рисунку показано такі компоненти:

- комп'ютерна плата Raspberry Pi 1b з цифровими, аналоговими інформаційними входами/виходами для запису та виходами для підключення живлення;
- модуль підключення камери вбудований в материнську плату міні-комп'ютера;

- пристрій, що робить знімок обличчя людини, а потім передає інформацію на міні-комп'ютер для обробки (також див. пункти 8 і 9 CSP);
- блок управління відкриттям дверей;
- частина датчика руху.

Схема плати Raspberry Pi (основного блоку з GPIO) має 27 цифрових, аналогових і послідовних входів, позначених від GPIO 0 до GPIO 27. Є додаткові входи 5 В і 3,3 В для живлення. Блок камери передає всю інформацію на плату через 8 інтерфейсів. Блок управління дверима містить транзистор, пару резисторів і сам привід.

Мініатюрний комп'ютер Raspberry Pi здатний обробляти як аналогові, так і цифрові сигнали. У проектах використовуємо його без додаткових компонентів для перетворення аналогового в цифровий або цифрового в аналоговий. Для живлення плати потрібна напруга 5 В і струм 1 А, але як тільки маємо зовнішні компоненти, такі як камери, датчики руху та виконавчі механізми, підключені до неї, життєздатним варіантом буде взяти блок на 2 А. Також знайшли проблему з приводом (дверний замок). Він повинен був працювати в ситуації живлення 12 В, що призвело до того, що в цьому випадку одну систему живлення було видалено, щоб мати дві із загальною землею. Для простоти схеми та необхідності комутатора було обрано джерело живлення на 12 В, а на лінії живлення мінікомп'ютера розміщено стабілізатор напруги на 5 В.

Процедура роботи схеми полягає в тому, що спочатку активується датчик руху, а потім цей сигнал передається на головну плату, яка далі ініціює програму згідно з розкладом. Таким чином, камера починає активуватися і знімати людину, яка стоїть перед нею. Пізніше це зображення буде передано для аналізу на борту. На останньому етапі позитивна індикація з табло активує виконавчий механізм. [41-50]

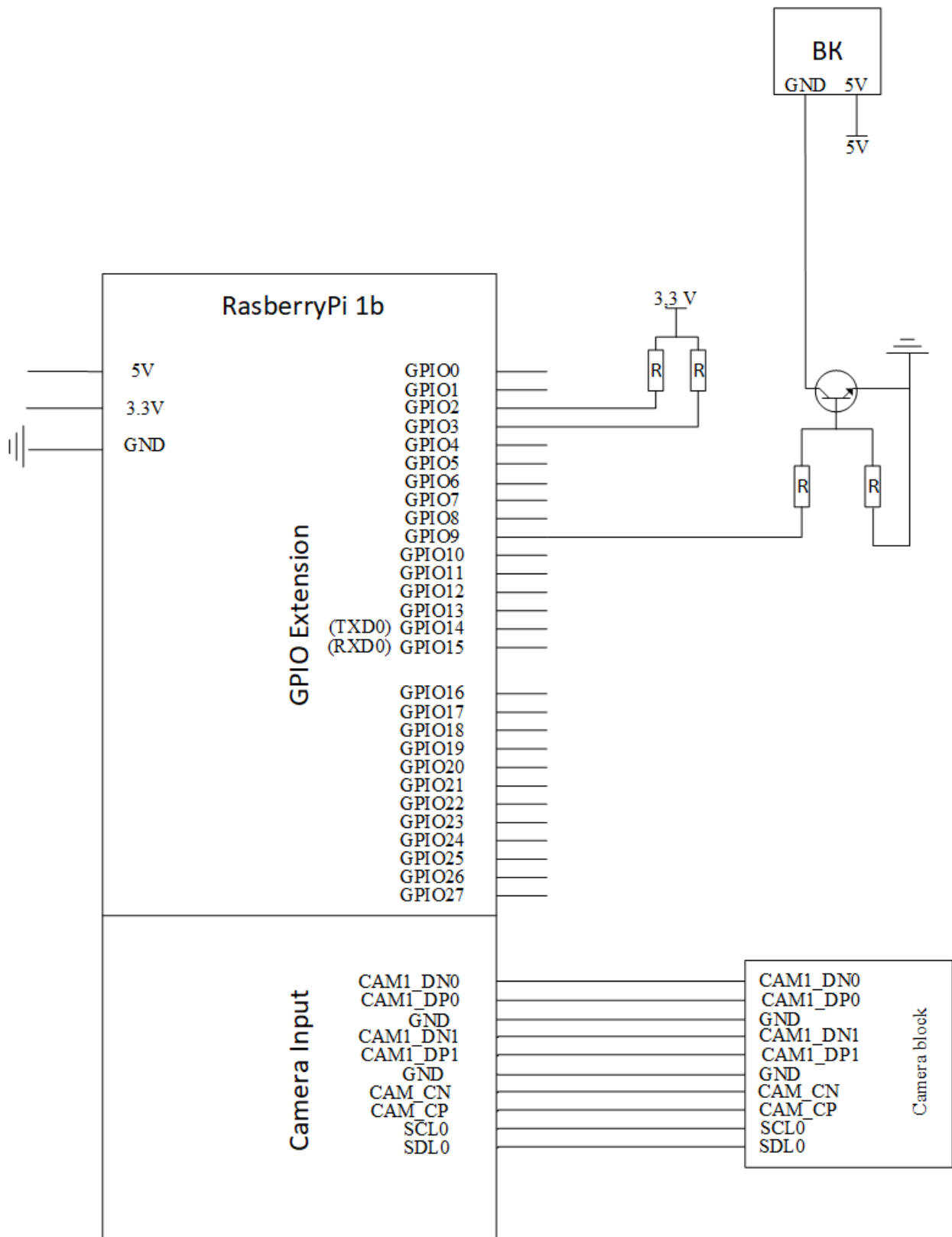


Рисунок 2.9 - Монтажно-комутаційна діаграма СККД

2.5 -Висновки до другого розділу

У другому розділі проведена розробка моделі автоматизації системи контролю та керування доступом. Наведено опис характеристик керування системою розпізнавання обличь. Виконане обрання платформи для створення локальної системи автоматизації. Зроблено проектування застосунку, а також обрання бази даних. Запропонована монтажно-комутаційна схема автоматизації СККД.

3 МОДЕЛІ АВТОМАТИЗОВАНОГО НАВЧАННЯ ЗАДАЧ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Для виконання поставленої задачі — створення автоматизованої системи контролю доступу людей — необхідна розробка математичної основи обробки зображень. Нині це питання розглядається як клас задач комп'ютерного зору, який має велику кількість прикладних задач.

3.1 Аналіз готових рішень

Сьогодні існує величезна кількість методів розпізнавання, кожен з яких має різні властивості, потенціал точності, швидкість і рівень надійності. За технологією, що використовується для розпізнавання, алгоритми розпізнавання поділяються на дві групи: 2D. Процес розпізнавання працює на якійсь точній формі людини (2D-технологія). Зображення є «плоскими», які використовуються для вивчення обличчя за текстурою, а певні ділянки на обличчі створюють високий контраст, який є дуже жорстким в умовах слабкого освітлення.

Він тривимірний. Ця технологія розвивається на структурі черепа (3 покоління). Системи 3D-розпізнавання набагато більш стійкі до проблем з освітленням, оскільки особливості будови черепа враховуються вже при створенні моделі людини.

Усі плюси 3D-розпізнавання стають плюсами, якщо швидкість обробки та пошук збігів вважаються недоліком, який не було правильно імплантовано. Крім того, технологія 3D-розпізнавання вимагає такої величезної обчислювальної потужності, а ціна обладнання для такого типу технології набагато вища, ніж для 2D-технології. Поки що в системах відеоспостереження використовуються ефективні алгоритми розпізнавання, засновані або на піксельних значеннях, або на характерних точках (вузлах карти обличчя).

Методи на основі пікселів залежать від кольору або яскравості для виявлення обличчя на зображенні. Основні з них: [51-60]

Фактично, Eigenfaces — це техніка, яку вперше представили Метью Терк і Алекс Пентланд у 1991 році, яка швидко стала найпопулярнішою для практичного розпізнавання облич. Загальна ідея алгоритму Eigenface полягає в представленні характеристик зображення обличчя як зваженої суми невеликого набору власних векторів. Потім алгоритм зіставляє профілі з шаблоном кадру, що зберігається в базі даних, і обчислює різницю між ними. Це ступінь відмінності, яким є коефіцієнт шаблону для відповідної пари. Eigenface — дуже хороший алгоритм, оскільки він працює майже щоразу за хороших умов освітлення. Fisherfaces є вдосконаленою технікою Eigenfaces і має кращу адаптивність. Він реєструє не тільки зміни при зміні світла, але й змінюється чутливість до міміки. Власне обличчя було наближенням обличчя Фішера. Тут апроксимація лінійності LDA призводить до максимізації лінійних дискримінантних змінних Фішера в сенсі коефіцієнта Фішера. Підхід Fisherfaces працює з даними, призначеними для максимального розділення класів зображень облич. У той час як власні грані вимагають, щоб проекція була чутливою насамперед до змін освітлення.

Метод LBP - просто дуже хороший спосіб розпізнавання обличчя. LBP кожного пікселя в зображенні набуває значення яскравості, яке околиці цього пікселя представлено певною функцією. Таким чином, зображення складається з областей, кожна з яких обчислюється за допомогою гістограми. Після об'єднання гістограми порівнюються за допомогою машинного навчання, для якого більш традиційна версія застосовує підхід найближчого сусіда. Монотонні зміни освітлення негативно впливають на алгоритм, що робить цей підхід не дуже хорошим для розпізнавання обличчя в системах реального часу, на відміну від EigenFaces.

Підходи на основі характеристик відрізняються від попередніх робіт тим, що вони оцінюють інтенсивність пікселів за ординатами характерних точок на

зображенні. Такими ознаками можуть бути, наприклад, центр очей, місце носа, довжина брів, губ і т. д. Такий підхід поєднує як моделі з активною зовнішністю, так і моделі з активною фігурою.

Її запропонували Тім Кутс і Кріс Тейлор у 1998 році. Активна модель зовнішнього вигляду — це статистична модель зображень, які можуть деформуватися за допомогою різноманітних трансформацій. 2D модель:

Він містить два типи параметрів: параметри форми та параметри зовнішнього вигляду, пов'язані з формою та визначені статистичною моделлю пікселів або текстур зображення. Обидва відповідають двом типам параметрів, визначених у статистичній моделі пікселів або текстур зображення. Модель має бути навчена на наборі зображень, позначених заздалегідь. Процес маркування зображень виконується вручну.

Модель активної форми (ASM) являє собою суто статистичне співвідношення антропометричних точок. Для кожного зображення є два варіанти параметрів; один набір стосується активних моделей зовнішнього вигляду, які зберігають параметри форми, а інший — це параметри зовнішнього вигляду зображення. Спочатку модель має бути навчена на наборі попередньо позначених зображень. Позначення зображень займає дуже багато часу. У ньому зазначено місце проведення антропометричних вимірювань. Узагальнений Прокрустовий аналіз координат зображення введений в єдину систему масштабування та центрування всіх точок). Тепер знайдіть середнє значення форми та коваріаційну матрицю для всього набору зображень. Потім отримують власні вектори коваріаційної матриці. Вони знову розташовані в порядку зменшення значень відповідних власних значень. Оптимізація забезпечує фіксацію розташування ASM у новому зображенні, яке не використовувалося під час навчання.

Не буде перебільшенням те, що за останнє десятиліття велика частина роботи в області комп'ютерного зору була повністю орієнтована на виявлення об'єктів, зіставлення форм і розпізнавання образів. Тому питання розпізнавання

об'єктів і облич за допомогою моделей машинного навчання не є першочерговим, і було описано огляд існуючих методів, їх плюси і мінуси, висвітлюючи плюси і мінуси вже реалізованих методів, враховуючи особливості, які актуальні для реалізації систем такого типу.

Автори в роботі [4] доводять, що для розпізнавання людини використовується багато біометричних методів. Розпізнавання очей і райдужної оболонки ока, розпізнавання відбитків пальців і розпізнавання обличчя є одними з них. Наприклад, одна з важливих частин людського обличчя необхідна для ідентифікації людини і надалі знаходить своє застосування в сферах безпеки та криміналістики. Це, у свою чергу, потребує належних методів виявлення та розпізнавання облич для нерухомих зображень або відеопослідовностей — щодо позування, оклюзії, старіння та роздільної здатності.

Автори працювали над синтезом облич, щоб прискорити та зробити розпізнавання більш точним за допомогою різних наборів даних облич, таких як ORL, YALE, AR, LFW. Автори пояснили різні типи методів розпізнавання облич і проблему підвищення ефективності та швидкості розпізнавання облич у великих базах даних і порівняли їх з точки зору точності та швидкості розпізнавання.

Він [6] підкреслює необхідність переналадження схем безпеки з виявленими недоліками та вразливістю існуючих заходів безпеки, відповідно.

Обидва методи автентифікації на основі бейджів і на основі паролів є незначними плодами для обходу. Біометрія – альтернативне можливе рішення, яке також має недоліки. Розпізнавання райдужної оболонки ока за допомогою сканування райдужної оболонки ока є дуже нав'язливим і точним.

Це широко прийнято, якщо особи не заперечують бути ідентифікованими, оскільки це дуже поширений стандарт автентифікації. На відміну від суворо контрольованого середовища, соціальна прийнятність,

надійність і ефективність досягають належного балансу з розпізнаванням обличчя.

Ці розділи мають на меті дати огляд сучасного 2D розпізнавання обличчя та підходів до 3D на основі моделі. Крім того, надаємо деякі табличні порівняння атрибутів для різних наборів даних, щоб допомогти перехресним посиланням на результати між роботами. Наприклад, такі параметри, як розмір вхідних даних, швидкість розпізнавання та кількість розв'язків для даного набору даних, створюють таблицю з переліком цих параметрів для різних робіт.

Автори [61] провели дослідження принципу «збільшення даних» для додатків розпізнавання обличчя. Результати показали, що глибокі згорточні нейронні мережі (DCNN) мають великий потенціал у розвитку розпізнавання обличчя. Такі DCNN вимагають величезних позначених вибіркового даних для навчання. Генерувати штучні дані дуже дорого та довго. Цим представляємо п'ять методів збільшення даних для зображень обличчя щодо зачісок, окулярів, поз, освітлення та орієнтирів.

Запропоновані підходи покращують набір тренувальних даних, щоб будь-які наслідки, згадані вище, виникали через неправильне розташування, зміни пози, зміни освітленості та часткові оклюзії, навіть переоблаштування під час тренування. Ефективність кожного методу розширення даних проілюстровано в порівнянні з базою даних Multi-PIE. Крім того, це порівняння також було виконано для баз даних LFW, YTF і IJB-A. Результати експериментів показують, наскільки запропоновані методи дійсно можуть вплинути на продуктивність розпізнавання обличчя.

Дослідження [62] виявило наступні проблеми з розпізнаванням обличчя:

- вигляд обличчя непослідовний
- фони різні
- освітлення для контрасту

Тепер розглянемо деталі. Обсяг інформації, отриманої на обличчі, є однією з двох основних помилок, пов'язаних із відповідним зображенням зображення, кутом повороту від відстані до очей тощо. Друге важливе значення — роздільна здатність зображення; певну точку (очі, губи, ніс). тощо) на еталонній карті або під час навчання, або під час процесу визначення облич. Це може викликати хибнопозитивні або хибнонегативні результати. Засіб полягає в тому, щоб взяти дані під деякими кутами, а потім сегментувати їх на відповідні блоки. Другим за значенням є рівень яскравості; Хоча це аналогічно оку в цифровому світі, практично вся ручна обробка зображень полягає в розрізненні кольорів між людським оком і розумом, і комп'ютер тут настільки чіткий. Потім ціле число зображення комп'ютера перетворюється в діапазон від 0 до 255 і вважається числовим значенням. Таким чином, контраст освітлення викликає різницю в значеннях пікселів, отже, розриває з'єднання в мережі. Найпростіший спосіб – це зробити зображення з подібними або меншими рівнями світла. Якщо ні, тобто якщо система працюватиме в земних або інших середовищах, то вона буде змушена перетворити зображення на атрибут класу іншого типу. Результат також залежить від походження даних зображення; це одне з простих питань. Алгоритм Box Bounding існує вже давно. Використовуючи контраст у своїх зображеннях, цей алгоритм може окреслювати різні об'єкти, навіть якщо він їх не ідентифікує. За допомогою рішення Google для розпізнавання та перевірки обличчя: FaceNet, експерти компанії оприлюднили своє розуміння проблеми та запропонували рішення, яке повинно бути гнучким і вирішувати деякі з вищезгаданих проблем.

3.2 Архітектурні особливості нейромережі FaceNet

Вибираючи з розглянутих рішень, було домовлено прийняти розробку нейронної мережі «FaceNet» як відправну точку, а потім переналаштувати її для запропонованого проекту. «FaceNet» — це цифрова мережа, створена Google

для розпізнавання обличчя. Він відображає вхідне зображення на представлення евклідового простору, стискаючи його згортками. На рис. 3.1 представлена принципова схема моделі FaceNet. [63-65]

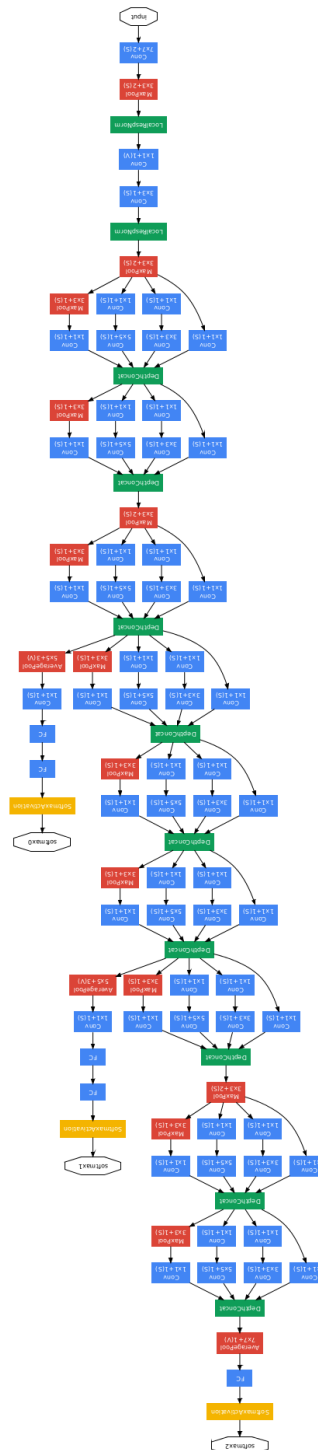


Рисунок 3.1 - Архітектура мережі FaceNet

На рисунку видно, що основними компонентами цієї архітектури є блок InceptionLayer, який є фільтром, який містить кілька згорткових шарів плюс максимальний рівень об'єднання. Математично це показано на рисунку 3.2.

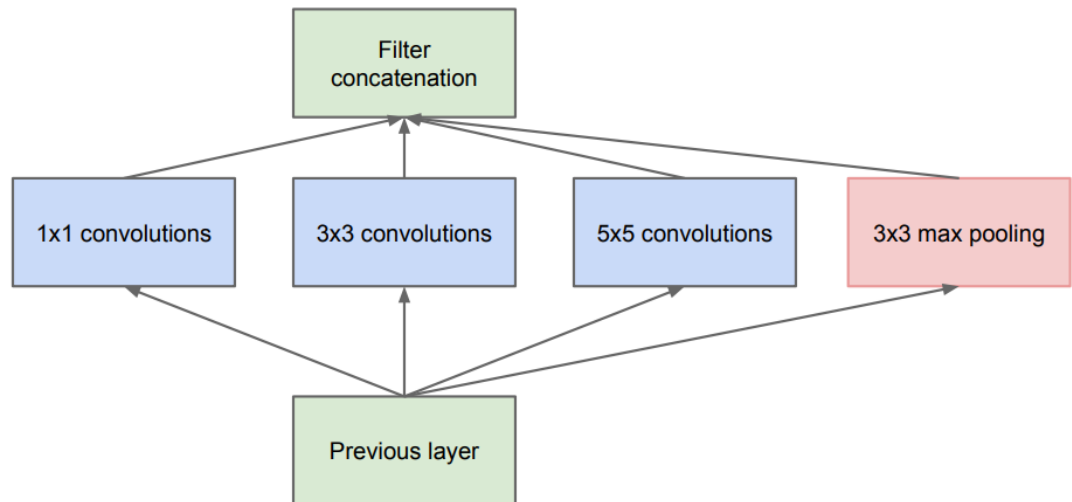


Рисунок 3.2 - Схема Inception Layer

Даний елемент архітектури складається із елементів (шарів) які будуть розглянуті нижче.

Згортка (конволюція) — це комплексна функція штучних нейронних мереж, яка формує глибоке навчання з проміжними технологіями для ефективності розпізнавання образів. Основна принципова ідея згорткових нейронних мереж — це послідовна альтернатива згорткових шарів. Можемо говорити про основний постачальник продуктивності для згорткових нейронних мереж як про згортковий рівень. Кожен канал попереднього шару бере участь у процесі згортки своїм фільтром, відповідальним за обробку частини зображення. Суттєвою властивістю згортки є те, що кількість відповідних досліджуваних параметрів досить незначна. Схематична діаграма процесу для згорткових шарів наведена на рисунку 3.3 нижче.

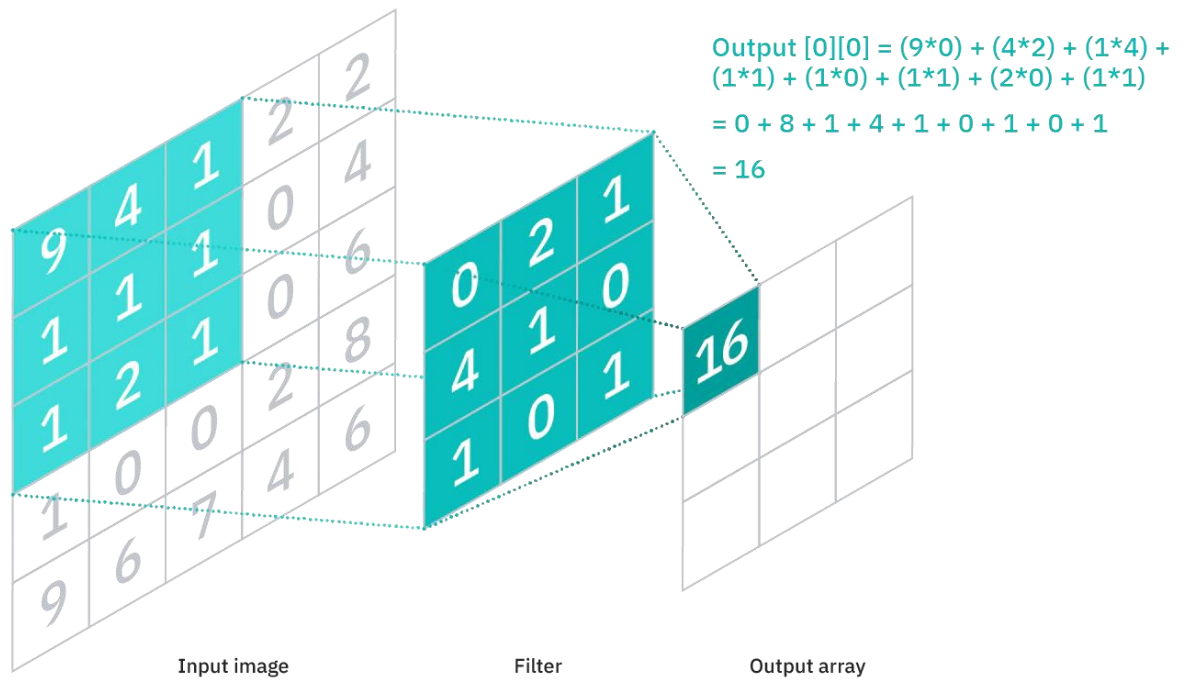


Рисунок 3.3 - Спрощене зображення функціонування згортки в computer vision

Максимальне об'єднання максимально об'єднує значення кожної частини матриці при скороченні ознак. За ним зазвичай слідує шар згортки. Це передбачає явне моделювання ознаки в результаті зменшення розмірності. Отже, незначні варіації в кількості даних не спричинять значного впливу на вихідні значення. Схема Max Pooling показана на рисунку 3.4.

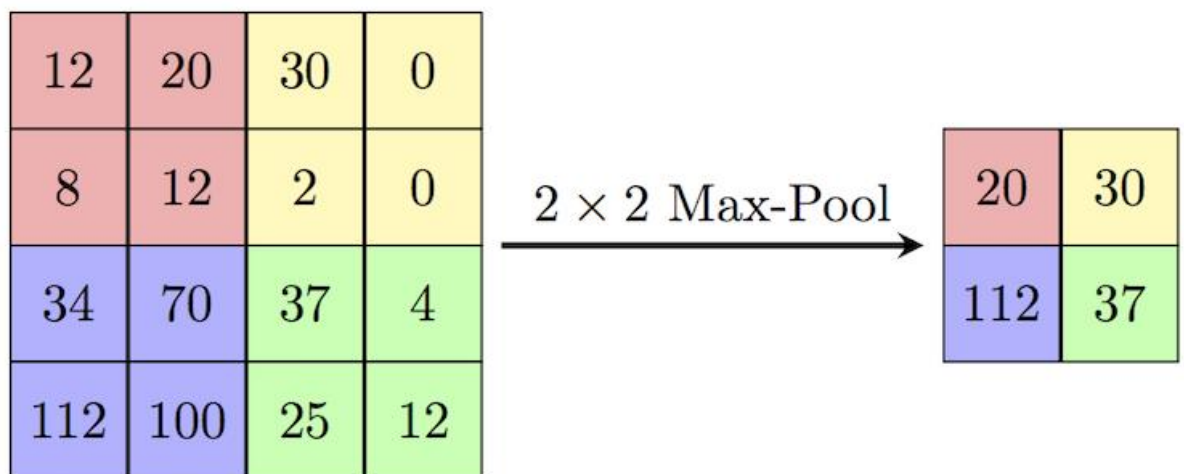


Рисунок 3.4 – Схематичне представлення роботи Max Pooling

SoftMax — це функція, яка перетворює вектор чисел у вектор значень ймовірностей. Згідно з цією формулою, ймовірність кожного значення є ймовірністю того, що це значення буде вибрано з усіх входжень значень у вихідному векторі. Ілюстрація того, як працює функція, показана на рисунку 3.5.

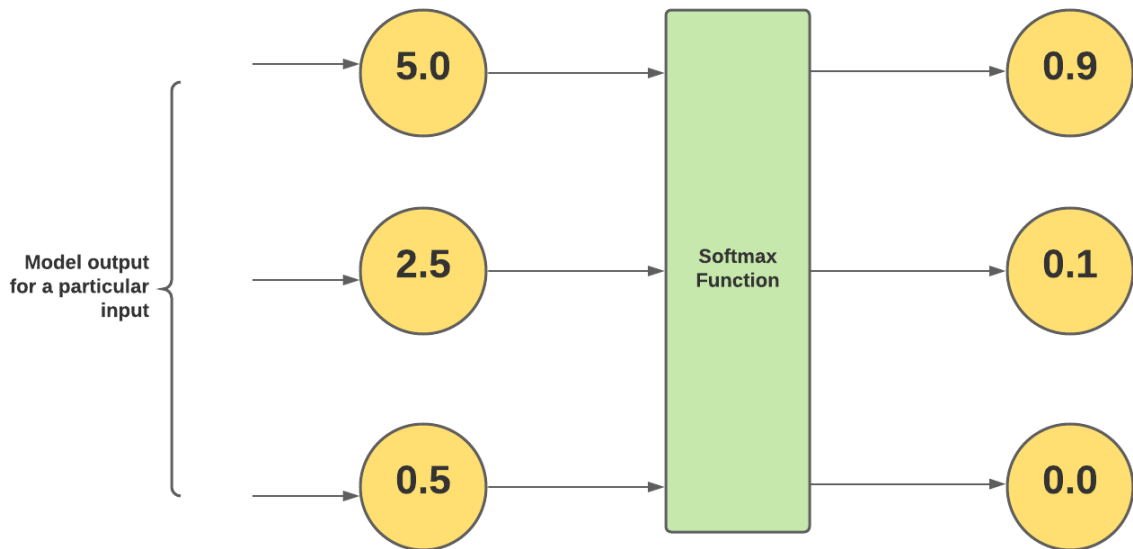


Рисунок 3.5 - Принцип функціонування функції активації SoftMax

Для найкращої роботи модуль «FaceNet» вміщує в собі додаткові компоненти, які представлено на рис.3.6.

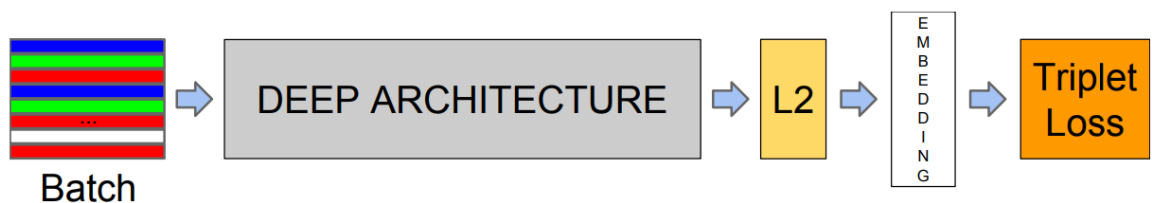


Рисунок 3.6 - Додаткові елементи що вміщуються в “FaceNet”

Додати текст до списку:

- Batch - навчальний набір пакетів зображень;
- набір функцій Deep Architecture- Inception Layer;

- нормалізація L2- L2;
- вбудовування – кінцеве перетворення зображення в евклідовому просторі;
- Triplet Loss - функція втрат для перенастроювання цілі навчання моделі.

Пакет – це коли весь набір даних розбивається на частини, оскільки обробка всього обсягу даних не підходить для кількох моментів, таких як швидкість вивчення моделі та точність завершення моделі.

L2 нормалізація — це техніка, застосована для зниження рівня повторного навчання моделі.

Потрійна втрата — реалізовано з тією ж метою, що й модель, яка використовує алгоритм «FaceNet» для зменшення відстані між подібними зображеннями: L2 нормалізація — це техніка, застосована для зниження рівня повторного навчання моделі.

Потрійна втрата — реалізовано з тією ж метою, що й модель, яка використовує алгоритм «FaceNet» для зменшення відстані між подібними зображеннями:

$$Loss = \sum_{i=1}^N \left[\|f_i^a - f_i^p\|_2^2 - \|f_i^a - f_i^n\|_2^2 + \alpha \right]_+$$

3.3 Аналіз поняття баз даних

Принципи систем підтримки прийняття рішень такі, що обробка транзакцій не настільки ефективна, тому дані, які почали аналізуватися, почали відокремлювати окремі бази даних; ці бази даних пізніше стали відомі як сховища даних або сховища інформації. У літературі також використовується англійський термін Data Warehouse. Батьком концепції сховищ даних

вважається Білл Інмон. Вплив Великий вплив на розвиток концепції сховищ даних мала американська корпорація ІВМ.

Концепція сховища даних – це концепція підготовки даних для аналізу, в якій забезпечується виконання наступних положень:

1) Інтеграція та координація даних з різних джерел: традиційних систем оперативної обробки даних, інформації з внутрішніх і зовнішніх джерел щодо організації, електронних архівів;

2) Поділ наборів даних, які використовуються системами обробки транзакцій і системами підтримки прийняття рішень

Концепція сховища даних. Архітектура бази даних для зберігання

Однією з гарячих тенденцій майбутнього зростання технологій реляційних баз даних і мови SQL є дедалі більше сприйняття сховищ даних і програм бізнес-аналізу. Процес агрегування даних допомагає в статистичній перевірці даних, аналізі тенденцій і прогнозуванні, з яких можна отримати цінні дані, що стосуються кореляції між діяльністю компанії та поведінкою її клієнтів. Data Warehousing підтримується реляційною СУБД.

Робота користувачів виконуватиметься паралельно, щоб отримати високий паралелізм для систем OLTP, які дозволяють кільком користувачам отримувати доступ до одного джерела даних одночасно та виконувати необхідну обробку даних. Системи OLTP призначені для вирішення різноманітних завдань, серед яких:

- введення даних, отриманих з транзакцій;
- усунення надмірності даних для високого рівня точності;
- забезпечення цілісності інформації та даних;
- створення спеціальних документів і звітів;
- підвищення ефективності процесу за рахунок паралельної обробки та оптимізації запитів.

Більшість із цих цілей стає можливим завдяки тому, що бази даних перебувають у третій нормальній формі.

Загалом системи OLAP вважаються класом інформаційних систем підтримки прийняття рішень та управління. Основна мета системи OLAP полягає в аналізі величезних обсягів детальних даних у всіх видах можливих представлень, узагальненні та агрегуванні даних різними способами з метою виявлення тенденцій, конкурентних переваг і оптимізації бізнес-діяльності.

Третя реляційна база даних нормальної форми не обов'язково повинна зберігатися в системах OLAP. Тільки таким чином ця форма повинна бути знищена, а база даних денормалізована в деяку розширену форму з такою надмірністю.

Усе це базується на тому факті, що інформація, яка зберігається в системах OLAP, змінюється нечасто. Дані зберігаються, щоб можна було обробляти їх для створення звітів, які допоможуть людям планувати майбутнє свого бізнесу.

База даних перейменована в просторову базу даних (вимірну базу даних) відповідно до якоїсь спеціальної схеми або структури. Це буде свого роду зміна окремого куба в окремих категоріях для аналізу бізнес-даних, таких як час і географічне розташування або лінійка продуктів і тому подібне. Зберігання згадується в різних програмах:

- для великого виробництва – аналіз трендів продажів; зокрема, якщо компанія може проаналізувати, в який сезон протягом року відбувається найбільший обсяг продажів, тоді було б набагато ефективніше спланувати виробництво, розвантажити склади та заощадити гроші;

- оптова торгівля - Аналіз ефективності заходів для підвищення продажів і демографічного профілю в поєднанні з факторами може виявити найкращі способи залучення потенційних покупців, заощаджуючи при цьому;

- телекомунікації – Аналіз моделей вхідних дзвінків від клієнтів може допомогти зробити ціни на пакети послуг дуже привабливими та залучити нових клієнтів від людей, які користуються подібними послугами в інших країнах;

- авіакомпаніям - аналіз схем руху пасажирів є основою для планування рейсів, тарифів і обсягів перевезень з метою максимізації прибутку компанії;
- фінансовим структурам - аналіз коефіцієнтів факторів за отриманням і погашенням кредитів від клієнтів, а також їх порівняння з попередніми роками детальніше дозволяє зробити висновки про кредитоспроможність клієнтів.

Структуру бази даних сховища даних потрібно буде побудувати так, щоб максимально спростити аналіз інформації. Дані мають бути зручно «розподілені» в різних напрямках.

Це структура бази даних зберігання не повинна бути реляційною, а скоріше просторовою базою даних (вимірною базою даних). Основною таблицею просторової бази даних є таблиця фактів. Її рядки називаються фактами та представляють виміряні показники події. Вимірювання дозволяють нам належним чином розділити ці факти за такими атрибутами, як час, продукт, клієнт і місцезнаходження клієнта. Просторові таблиці стосуються даних у таблицях фактів.

Інформація в сховищі бази даних найчастіше має форму (N) -вимірної куба фактів, що відображають господарську діяльність, яку веде компанія в певний час.

Кожна його клітинка представляє один факт - суму продажу в доларах. Місяці, які відповідають продажам, показаним на кубі, розташовані вздовж однієї грані куба. Другий вимір — категорії продуктів. Третє – регіони збуту. Кожна клітинка містить обсяг продажів для відповідної комбінації значень для всіх трьох вимірів.

Фактичні програми використовують набагато складніші куби з десятками чи більше розмірами. Тим не менш, незважаючи на те, що 12-вимірний куб може бути досить складним для візуалізації, принципи організації такі ж, як і тривимірні. Кожен вимір означає певну змінну, що аналізується. Кожній комбінації значень усіх вимірів відповідає одне значення певного параметра – факт.

Розглянемо приклад для оцінки роботи типового аналітичного додатку. Припустімо, що це комерційний бізнес, який продає різноманітні товари від різних виробників кільком сотням клієнтів у різних регіонах країни. Керівництво хоче отримати аналіз тенденції продажів за п'ятьма аспектами на даний момент і рекомендації щодо подальшого збільшення продажів на основі цих даних. Ось аналізовані розміри, які визначають куб даних, подіями для якого є обсяги продажів:

1. Категорія. Категорія, до якої належить товар. Репозиторій містить інформацію про 24 категорії товарів.

2. Виробник. Ідентифікація виробника товару. Він може продавати товари 50 різних виробників.

3. Клієнт. Кому продається товар. Компанія має базу з трьохсот покупців.

4. Регіон. До якої країни регіону здійснюється продаж. Розглядалися три регіони.

5. Місяць. Керівництво компанії вирішило зберігати дані протягом 36 місяців для проведення порівняльного аналізу.

Результуючий куб даних містить 38880000 комірок ($24 \text{ категорії} * 50 \text{ виробників} * 300 \text{ клієнтів} * 3 \text{ регіони} * 36 \text{ місяців} = 38880000$).

У N вимірах зіркова схема найбільш ефективно представляє куб фактів більшості вітрин даних. Давайте розглянемо впровадження просторової бази даних для цього завдання аналізу на цьому OLAP і що це передбачає для нас. Кожен вимір куба містить таблицю, яка позначає значення цього виміру в цьому випадку, п'ять таких таблиць: КАТЕГОРІЇ, ПОСТАЧАЛЬНИКИ, КЛІЄНТИ, РЕГІОНИ та МІСЯЦІ. Кожна таблиця має один рядок, що відповідає кожному значенню вимірювання. Наприклад, таблиця MONTHS має 36 рядків — по одному для кожного місяця всього періоду, за який аналізуються дані продажів. Три регіони із загальної кількості регіонів представлені в таблиці REGIONS трьома рядками.

У зірковій схемі таблиці вимірювань часто мають стовпці з описовою текстовою інформацією або іншими атрибутами, пов'язаними з деякими конкретними вимірюваннями, як-от ім'я контактної особи від виробника, адреса та номер телефону клієнта або контактні лінії, які створюються за допомогою аналітичного аналізу. додаток.

Перший вимір – за його фактичним значенням або описом; наприклад, PRODUCT_NAME (наприклад, «Взуття» тощо) і MONTH. Інші два виміри будуть індексовані кодами – поле CUST_CODE у таблиці CUSTOMERS і поле SUPP_CODE у таблиці SUPPLIERS.

Найбільшою таблицею в базі даних є таблиця фактів. Це так просто. У цьому випадку це таблиця SALES. Передбачається, що таблиця фактів зберігає заходи, які знаходяться в клітинках N-вимірного куба. Крім того, він містить зовнішні ключі до всіх таблиць розмірності. У цьому прикладі їх п'ять. Кожен рядок у таблиці фактів відповідає одній клітинці в кубі даних. Існують також інші зовнішні ключі, які об'єднуються в цю таблицю, пов'язуючи її з таблицями вимірювань у позиції куба та значенні першого стовпця. Таблиця фактів неширока, але завжди довга: сотні тисяч і навіть мільйони у повноцінних сховищах даних у промислових і комерційних компаніях. Таблиця фактів завжди містить стовпці фактів, тобто числові значення, представлені у вигляді грошових значень і проданих кількостей тощо. Більшість звітів, які надходять із аналітичних програм, є лише зведеннями. Це суми, середні значення, максимуми та мінімуми або відсоткові співвідношення, отримані арифметичними операціями над числовими значеннями у стовпці фактів.

Розмірна модель дозволяє швидко виконувати аналітичні запити, але не підходить для зберігання великої кількості даних. Реляційна модель, з іншого боку, має невеликі обмеження щодо кількості даних, які можна накопичувати; однак СУБД, засновані на цьому, не забезпечують такої швидкості виконання аналітичних запитів.

Ситуація така, що вся інформація, яка міститься на складі, досить рідко запитується для аналізу. обмеження, властиві багатовимірним СУБД. Саме під час цього процесу виникає ідея відокремлення лише тих даних, які дійсно потрібні для конкретних аналітичних застосувань - в один набір від інших - і які можуть бути втілені в багатовимірній базі даних як її джерело з центрального сховища організації .

Таким чином, якщо порівнювати з виробництвом і реалізацією продукції, то багатовимірні бази даних працюють як невеликі склади. Від концепції компакт-диска вони називаються вітринами даних. Сховище даних - це спеціальне тематичне сховище, спеціалізоване для одного з видів діяльності організації. Логічна схема СППР буде використовувати центральний HR організації та вітрини даних аналітичних відділів.

Така система дає змогу скористатися можливостями реляційної СУБД для ефективного зберігання масивних даних і багатовимірної СУБД для швидкого виконання запитів підтримки прийняття рішень.

Дані завантажено в сховище. Користувачі-аналітики отримують доступ до нього за допомогою клієнтських програм, які можуть бути програмами трансляції запитів споживачів інформації або виконувати аналітичну обробку даних у сховищі. На відміну від систем оперативної обробки даних у СППР, які застосовують концепцію КД, критерії пошуку складу інформації, що видається у формі звіту, не фіксуються на момент її розробки; скоріше користувачі зазвичай працюють із нерегульованими запитами (спеціальними запитами).

У цьому випадку завданнями використання концепції сховища даних у СППР є:

- 1) Своєчасне надання аналітикам усієї аналітичної інформації, необхідної для прийняття обґрунтованих рішень;
- 2) Побудова консолідованої моделі даних організації;

3) Формування єдиної інформаційної бази, що забезпечує нескладний підхід до різноманітної інформації, що забезпечує отримання ідентичних відповідей на ідентичні запити від різних аналітичних підсистем. [63-65]

3.4 Висновки до третього розділу

У цьому розділі було розглянуто дослідження існуючих систем розпізнавання осіб, їх плюси і мінуси, дизайн і особливості додатків. Було проведено аналіз цього, щоб знайти найбільш відповідний дизайн для впровадження, що призвело до рішення використовувати FaceNet. У цьому розділі детально описані всі частини цієї архітектури.

4 ОПТИМІЗАЦІЯ ЧАСТИНИ СККД ПОШУКУ

Використання FaceNet як екстрактора допомогло представити зображення людини у вигляді багатовимірного вектора, в даному випадку розмір вектора 1×200 . Завдяки відображенню двох векторів — одного, що дає абстрактне зображення людини, а другого — зображення, яке зараз обчислюється, можна визначити, чи пов'язане довільне зображення з конкретною людиною. У результаті виникає питання про реалізацію методів векторного порівняння. Які існують підходи до визначення подібності отриманих векторів? Зверніться, будь ласка, до сучасних підходів у відповіді на це запитання. Обговорення на частини: кластеризація та більш поширений пошук усередині кластерів. Які різні методи кластеризації будуть використовуватися при розробці алгоритму запису?

4.1. Робота із векторами даних FaceNet

Зазвичай отримані вектори оцінюють на схожість. В даний час таку перевірку можна зробити шляхом обчислення косинусної подібності або евклідової відстані між запланованим і поточним векторами.

Косинусна подібність (англ. Cosine similarity) — це термін, що описує подібність між двома векторами: тим важливіше, чим ближчі два кути, враховуючи обчислення косинуса між цими двома векторами. Будучи оціненим як 1 для кута нуль градусів, усі інші кути, що належать до встановленого діапазону $(0, \pi]$, будуть додатково зменшеними значеннями. Це фактично є наближенням для напрямку, а не величини, два вектори, обидва спрямовані в одному напрямку, будуть мають косинусну подібність, рівну 1, тоді як для двох векторів, які утворюють один з одним кут 90° , буде мати нульову подібність; буде мати подібність рівну -1 незалежно від довжини векторів. [66-68]

Косинус пари ненульових векторів можна розглядати як їх скалярний добуток у просторі:

$$\mathbf{A} \cdot \mathbf{B} = \|\mathbf{A}\| \|\mathbf{B}\| \cos \theta$$

Для двох заданих векторів що мають ознаки, \mathbf{A} і \mathbf{B} , існує косинус подібності, $\cos(\theta)$, що обчислюється як скалярний добуток двох векторів і представляє довжину як

$$\text{подібність} = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}},$$

Евклідова відстань є найпоширенішим показником відстані. Евклідов простір – це, по суті, звичайний геометричний простір, який вивчають у класах математики, зазвичай пов'язаний із трьома вимірами. Зокрема, це може стосуватися будь-якого важливого інтегрального виміру. Евклідова відстань між двома точками така, що найкоротший шлях у евклідовому просторі. Насправді цей термін походить від Евкліда, якого інші люди свого часу називали «батьком геометрії», тому що це поняття існувало лише у нього. Пізніше у фізиці та математичній літературі були описані інші простори, такі як простір Афінів. У тривимірному просторі евклідової відстані цей найкоротший шлях проходить між двома заданими точками. Оскільки це найкраща метрика відстані, спочатку зосередимося на використанні дво- та тривимірного евклідового простору для визначення відстані між точками. Зазвичай евклідова відстань в основному використовується при моделюванні тривимірних світів. Так само в машинному навчанні це популярне як метрика відстані, де використовуються K -найближчі сусіди. Загалом, евклідова відстань, як правило, відображатиме, наскільки дві точки даних подібні за

припущенням, що з іншої інформації вже відомо, на яких ознаках базується кластеризація.

Це математична формула для обчислення відстані між 2 точками у 2D просторі за формулою Ейклінга:

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2}$$

Формулу легко перетворити, щоб був врахований 3D-простір, а також розв'язати проблему будь-якого розміру:

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + (q_3 - p_3)^2}$$

Загальна формула може перетворитись до виду:

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + \dots + (q_n - p_n)^2}$$

Однак описані вище підходи мають кілька проблем. По-перше, зі збільшенням кількості людей, які використовують систему, збільшується кількість оригінальних векторів, які потрібно зберегти, щоб порівняти їх із поточним вектором, і кількість операцій, які виконуються для порівняння обох.

Щоб зменшити кількість кроків, пов'язаних із запуском запропонованої системи, слід зробити наступне: налаштувати початковий набір векторів перед запуском, спочатку визначити, чи цей вектор, який зараз досліджується, є частиною кластера, а потім шукати кластер для запуску якому воно належить.

У результаті, якщо розмірність вихідних векторів вибірки дорівнює 100, то для перевірки одного з етапів перевірки потрібно виконати 10 000 процедур.

Якщо є 10 кластерів за цим методом вище, існує 1 процедура для підрахунку членства в кластері та 1000 процедур перевірки.

4.2 Кластеризація векторів

Кластеризація — це процес групування набору об'єктів таким чином, щоб об'єкти в одній групі (званій кластером) були більш схожі один на одного, ніж об'єкти в інших групах. Кластеризація — це математична техніка, яка використовується у багатьох відношеннях у різних галузях дослідження: одна з них — у науці, наприклад, біології та фізіології; інший застосовний у сферах маркетингу, таких як соціальні медіа та оптимізація пошукових систем; і третій — у сфері правосуддя, що стосується закону та порядку та запобігання злочинам.

Під час аналізу даних для обчислення навчальних даних алгоритм K-means спочатку починає з вибору набору центроїдів для кожного кластера та бере перший набір як центроїди випадкового вибору для початкових точок. Потім він обчислює центроїди, повторюючи процес ітерацій оптимізації положень центроїдів.

Перше завдання полягає в рівномірному розподілі будь-якої довільної кількості n -вимірних точок між k кластерами. Алгоритм процедури наступний:

Визначаючи кількість кластерів.

Вибір K випадкових точок або центрів (це відрізнятиметься від вихідного набору даних).

Для кожної точки даних у наборі даних призначте цю точку найближчому центру з K центрів. K -центри формуватимуть попередньо визначені K -кластери.

Обчислити дисперсію для кластерів і зсунути новий центроїд для кожного кластера.

Повторіть крок 3, щоб він включав перепризначення кожної точки даних новим найближчим центроїдам для кожного кластера.

Якщо обмін був успішним, досягнете кроку 4, інакше досягнете фінішної прямої.

Отримання готової моделі.

Останні варіанти для створення та вдосконалення кластерів, коли:

Центроїди досягли стабільності: їхні значення не змінилися після того, як кластер був успішним.

Задана кількість ітерацій досягається.

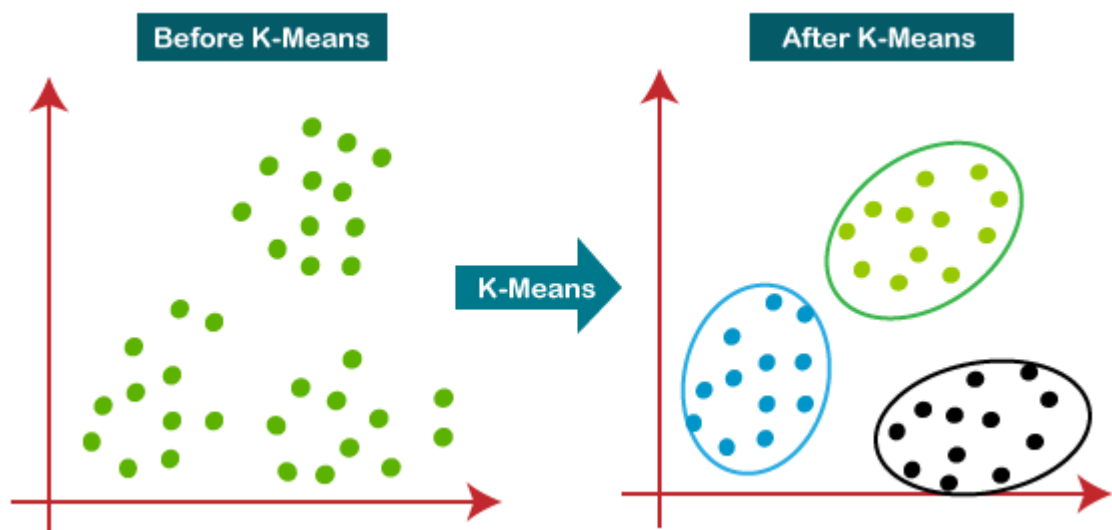


Рисунок 4.1 -Алгоритм роботи за методом к - середніх

Алгоритм К-середніх є дуже ефективним, якщо він формує високоефективні кластери. Але підібрати потрібну кількість кластерів – це серйозне завдання. Існує кілька різних підходів до визначення кількості кластерів, але обговоримо найефективніший метод визначення кількості кластерів, тобто значення К. Тому знаходження правильної або оптимальної кількості цих кластерів є дуже важливим.

Метою ієрархічної кластеризації є групування об'єктів у набір пов'язаних кластерів. Він починається з n кластерів, розглядаючи кожне спостереження як

один кластер. Потім він групуватиметься на кожному кроці ітерації — два найближчі кластери або кластеризація, яку найбільш доцільно об'єднати на цьому конкретному кроці процесу. Це триватиме безперервним об'єднанням щойно визначених кластерів в один кластер, поки не залишиться лише один кластер. Це показано на рисунку 4.2.

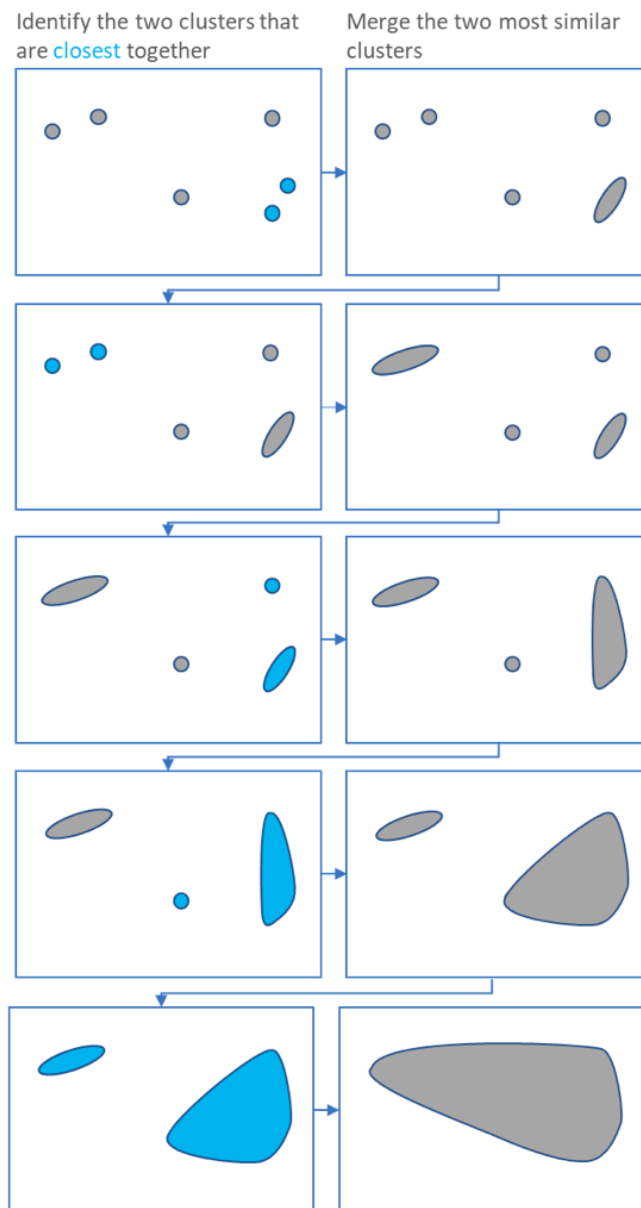


Рисунок 4.2 - Приклад функціонування ієрархічної кластеризації

Щоб зрозуміти популярність ієрархічного методу, важливо розуміти, що після його поділу на кластери створюється дерево зв'язків, а на рис. 4.3. ієрархії.

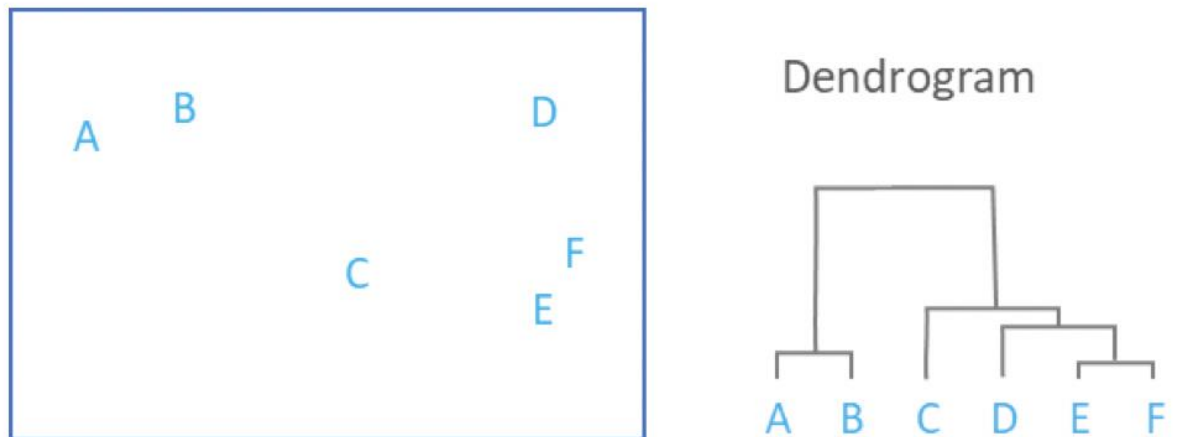


Рисунок 4.3 – Блок-діаграма ієрархії

Після перевірки це призводить до дерева, яке визначає право власності та повноваження у формі батьківського та дочірнього елементів. Відстань між будь-якими двома кластерами визначається шляхом проведення прямої лінії від одного кластера до іншого та обчислення довжини між двома точками. Це зазвичай називають евклідовою відстанню. Було подумано про інші показники відстані. с

Вибір метрики відстані повинен базуватися на теорії в конкретній галузі дослідження. Таким чином, міра відстані повинна служити меті визначення подібності у спосіб, який підходить для галузі дослідження. Наприклад, при об'єднанні місць злочину в межах міста має відігравати роль відстань між кварталами. Або, по суті, відстань між кожною точкою. Оскільки немає теоретичного обґрунтування іншого виду, за домовленістю використовується евклідова відстань, оскільки це найчастіший спосіб вимірювання відстані в реальному світі.

Порівняння методу k-середніх з ієрархічною кластеризацією. Однією з таких відмінностей є те, що ієрархічна кластеризація не така ефективна з великими обсягами даних у кластері, як k-середні. Причина полягає в тому, що час обчислення для алгоритму є лінійним для методу k-середніх і квадратичним для ієрархічного методу.

Що стосується кластеризації k-середніх, алгоритм просто почне будувати центр кластера на основі випадкових початкових точок, вибраних для вибірки. Це означає, що виконані результати під час кількох ітерацій алгоритмів можуть показувати певні відмінності між ними. Отже, йому бракує не лише відтворюваності, але й швидкості щодо точності генерування кластерів. Таким чином, це слід виконати кілька разів і розглянути найбільш прийнятне повторне рішення. Крім того, у випадку ієрархічної кластеризації отримані результати можна відтворити, що робить цей підхід більш придатним для великих вибірок. Це було б більш доречним, тому що, припускаючи, що кластери точні та чітко описують групи, до яких вони належать, цей кластер буде найкращим. З дизайну центральної точки методу k-середніх можна зробити висновок, що цей метод ефективний під час роботи з гіперсферичними формами кластерів (наприклад, двовимірне коло чи тривимірна сфера). Набагато кращу ефективність розпізнавання шумових даних порівняно з ієрархічним методом демонструє метод k-середніх, тому для цієї мети стандартним вибором є метод DBSCAN.

DBSCAN означає просторову кластеризацію додатків із шумом на основі щільності. Це важливий алгоритм, який використовує k-середні в моделях заміни. Під час неконтрольованого навчання він визначає різні класи точок даних на основі ідеї, що кластер — це область із високою щільністю даних, оточена областю з низькою щільністю, яка, у свою чергу, оточена областю з низькою щільністю. DBSCAN є основним методом кластеризації на основі щільності. Це може ідентифікувати кластери різних форм і розмірів із великих наборів даних із шумом і викидами.

Етапи алгоритму

- постійно вибирає випадковим чином точку з набору даних (єдина умова: кожна точка в наборі даних ще не була відвідана);
- якщо принаймні точки «minPoint» розташовані на відстані меншій або дорівнює «ε» від точки, усі ці точки вважаються частиною одного кластера;
- збільшуйте кластери шляхом багаторазового обчислення околиць для кожної суміжної точки тощо.

Алгоритм К-середніх може кластеризувати непрямо пов'язані точки. Навіть два спостереження, які знаходяться так далеко одне від одного у векторному просторі, зрештою опиняться в одному кластері. Оскільки кластери визначаються середнім значенням або центроїдом, що визначає кожен кластер, кожна окрема точка даних вкладає свої два центи у формування кластерів. Отже, навіть невелика зміна даних може потенційно змінити результати кластера. Однак це значно зменшується в DBSCAN самим способом виникнення кластерів. Для практичних цілей це, швидше за все, не викликає занепокоєння, якщо ви точно не знаєте, що маєте справу з аномальними даними.

Ще одна проблема з k-середніми полягає в тому, що нам потрібно знати кількість кластерів ("k"), щоб їх використовувати. Загалом не маємо попередньої інформації про те, що таке прийнятне значення k.

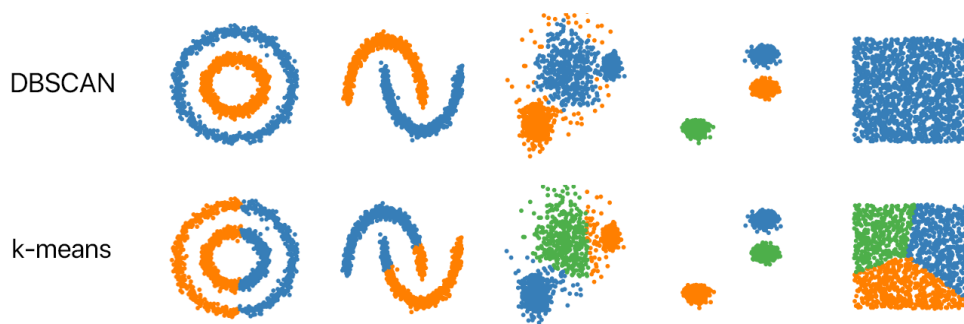


Рисунок 4.4 - Відмінності у функціонуванні методів k-середнє та DBSCAN

DBSCAN має більший успіх у різних популяціях, ніж kmeans.

Одна хороша річ полягає в тому, що перше припущення щодо кількості кластерів не потрібне для цього підходу, але слід змінити ще два параметри, щоб `eps` і `min_samples` показали успішний результат: перший згаданий параметр — це максимальна відстань між двома точками, яку слід враховувати. їх у сусідстві, а інше — це мінімальна кількість точок у сусідстві (інший числовий опис того, скільки членів має кластер), щоб екземпляр даних був частиною кластера. [70]

4.3 Дослідження роботи підходу до оптимального пошуку

Для простоти представлення розглянемо випадок, коли початкова точка для вихідних векторів складається з 200 екземплярів, з одним виміром, див. рис. 4.5.

Для прямого перерахування він повинен обчислити відстань до поточного вектора, який розглядається з кожним із вихідних екземплярів, за допомогою чого буде визначено значення мінімальної відстані. Рис. ілюструє блок-схему.

При використанні запропонованої методики слід визначити, чи належить поточний вектор до одного з кластерів. В результаті в просторі вихідний набір даних буде розділений на відповідні кластери, див. рис. 4.6.

Якщо вихідні вектори не були попередньо згруповані, тоді для всіх векторів, які належать до цікавого кластера, обчисліть відстань до поточного вектора, який, як очікується, буде в цьому самому кластері для кожного вихідного екземпляра цього кластера. Якщо відстань мінімальна, вважайте її такою.

Ефективність і здійсненність підходу потребують кількох досліджень. Особливо швидкість підходу слід перевіряти на різних розмірах вибірки та кількості кластерів, щоб побачити, наскільки він швидкий чи повільний.

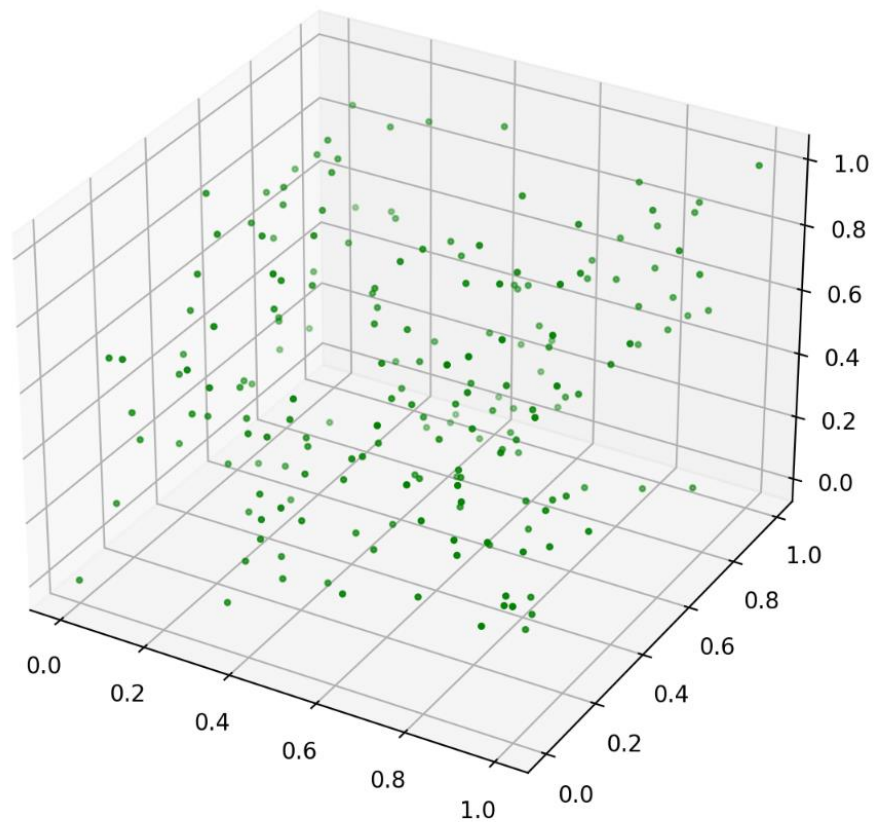


Рисунок 4.5- Уявлення початкових даних

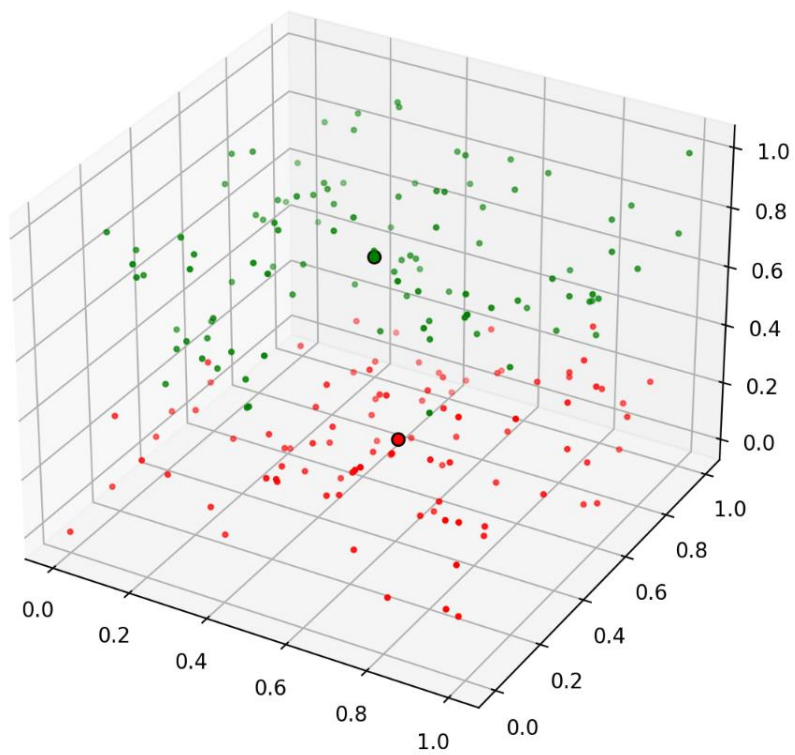


Рисунок 4.6 - Результати кластеризації (а)

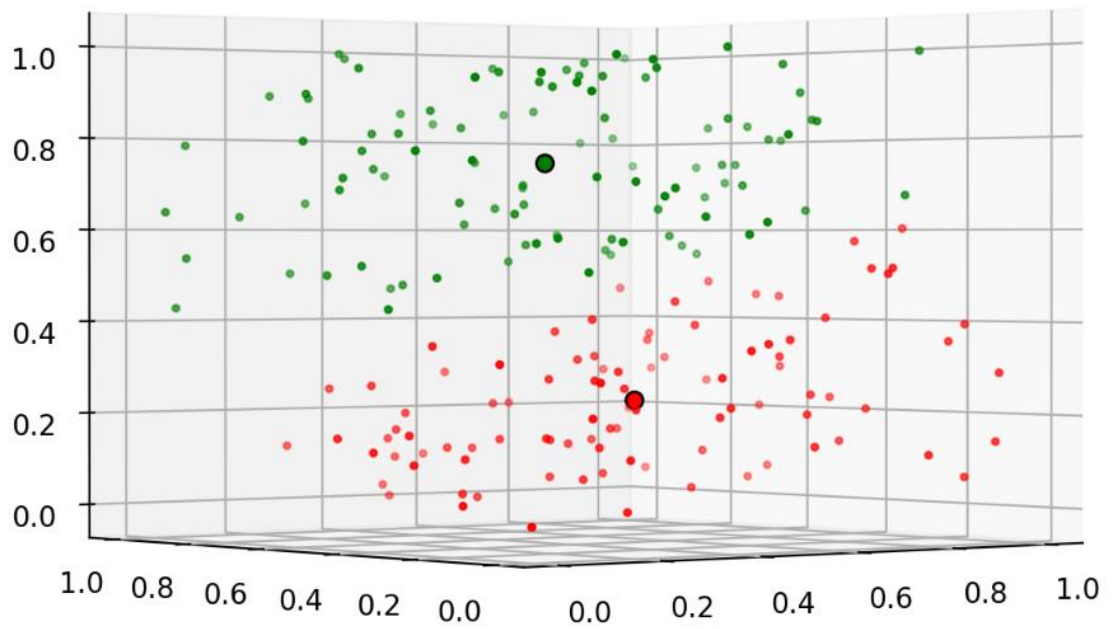


Рисунок 4.7 - Результати кластеризації (б)

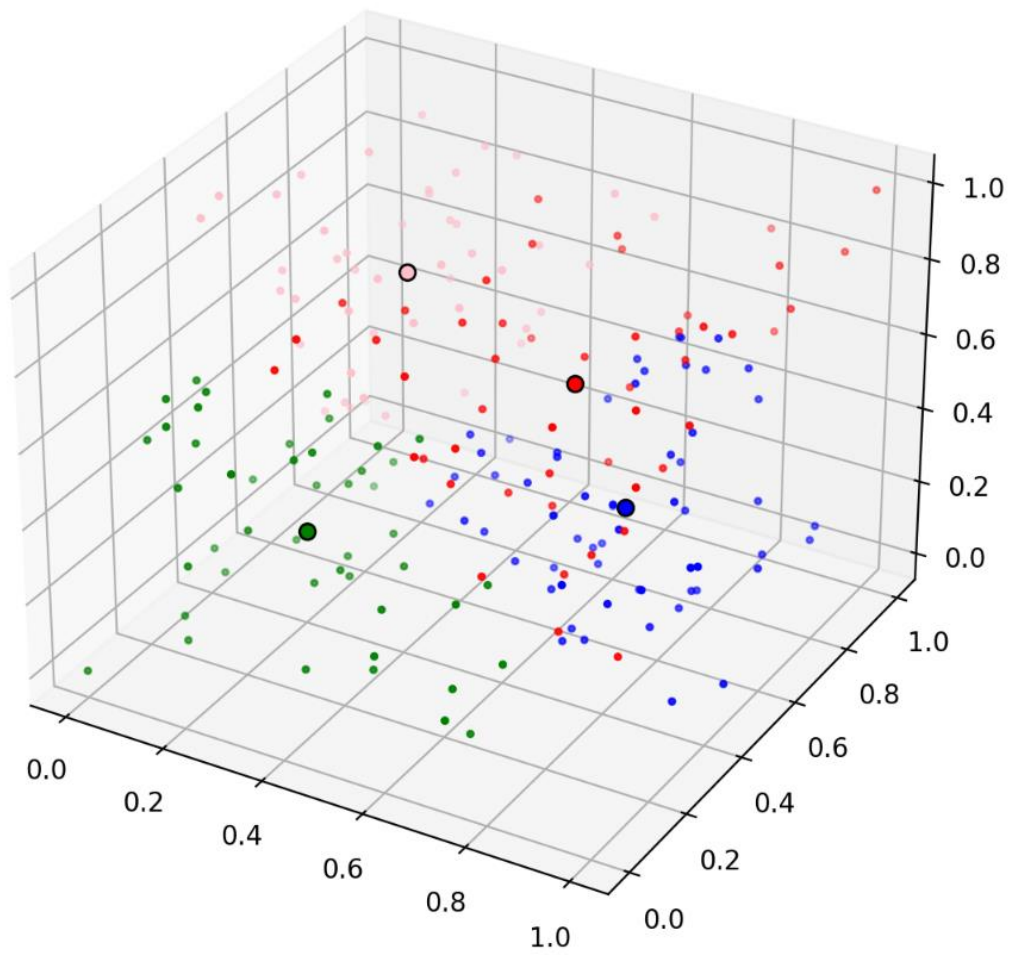


Рисунок 4.8 - Результати кластеризація (в)

Методологія дослідження 1: Вектор розміщується першим у просторі вибірки в деякому випадковому місці. Розпочинається пошук найбільшого схожого вектора, який має тестовий вектор у 0,99 значних координатах. У разі успіху реєструється час, витрачений на виконання пошуку. Потім це робиться з більш широкими популяціями. Це робиться з початковим розміром вибірки 1000, зменшуючи до 100 000, при цьому кластери зберігаються на рівні 2.

Результати досліджень див. на рисунку 4.9. продемонструвати велику цінність запропонованого підходу на більшій вибірці, створеній з 5000 унікальних екземплярів. Варто звернути увагу на діапазон 0-300, в цьому діапазоні підхід ефективний. Результати показали прямий зв'язок із швидкістю системи та розміром вибірки. [70]

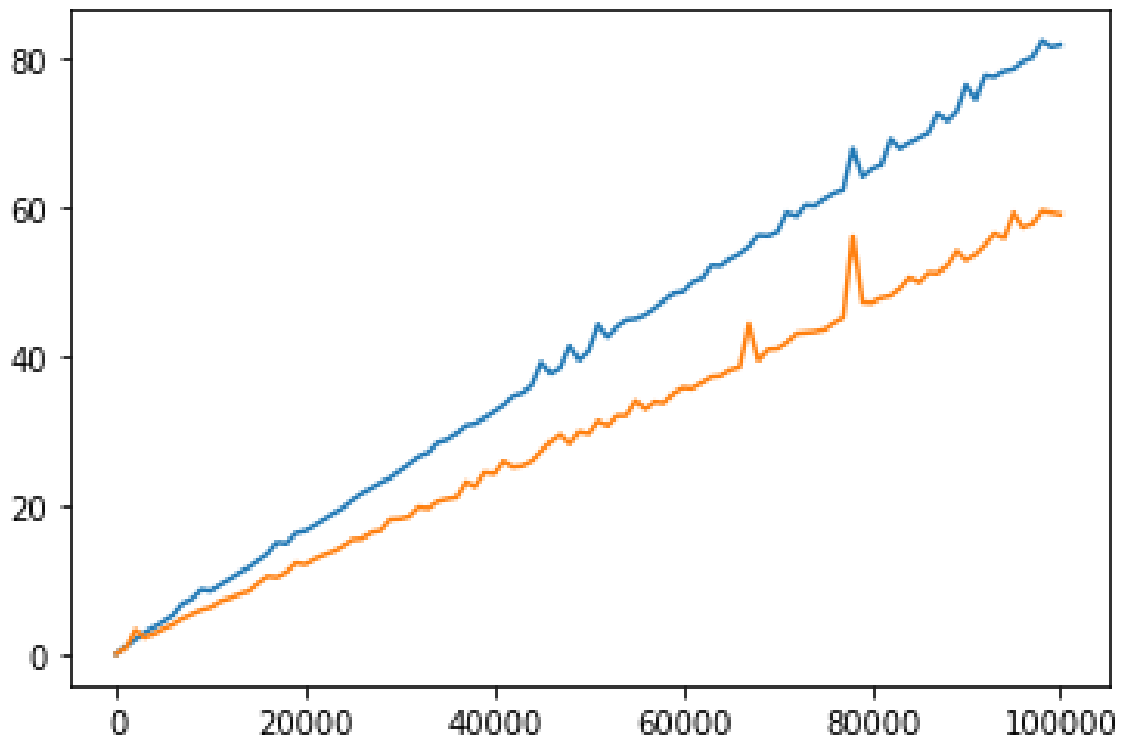


Рисунок 4.9 - Залежності від часу обчислення від величини вибірки

Дослідження 2 проводиться, коли кількість кластерів зменшується з 2 до 60, і все ще оцінюється в 200 000. Результати наведені на рис. 4.10.

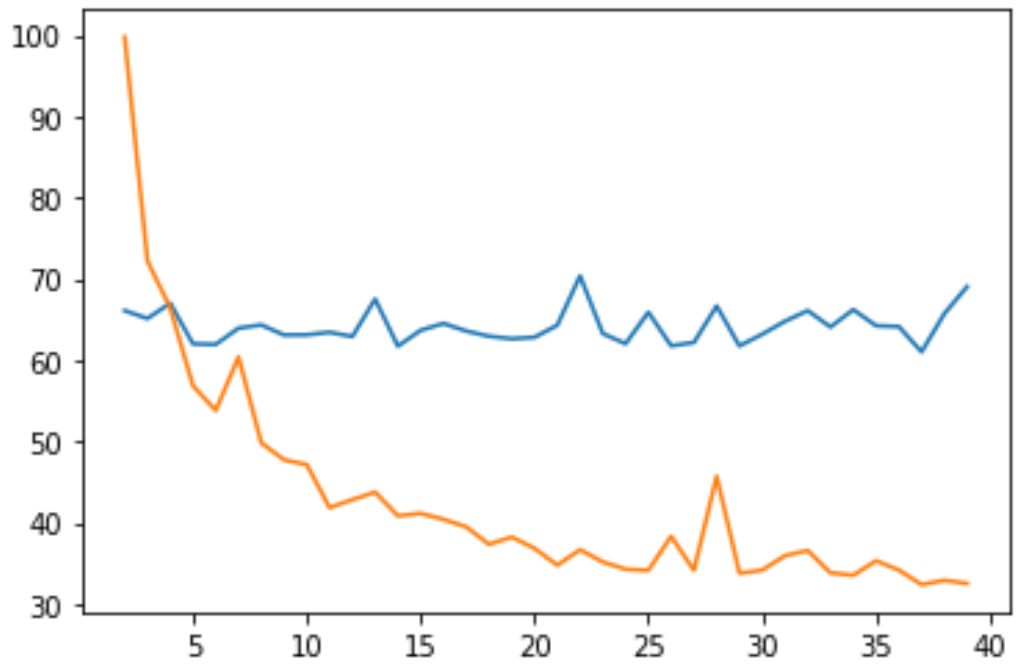


Рисунок 4.10 - Залежності від часу обрахунку від кількості кластерів

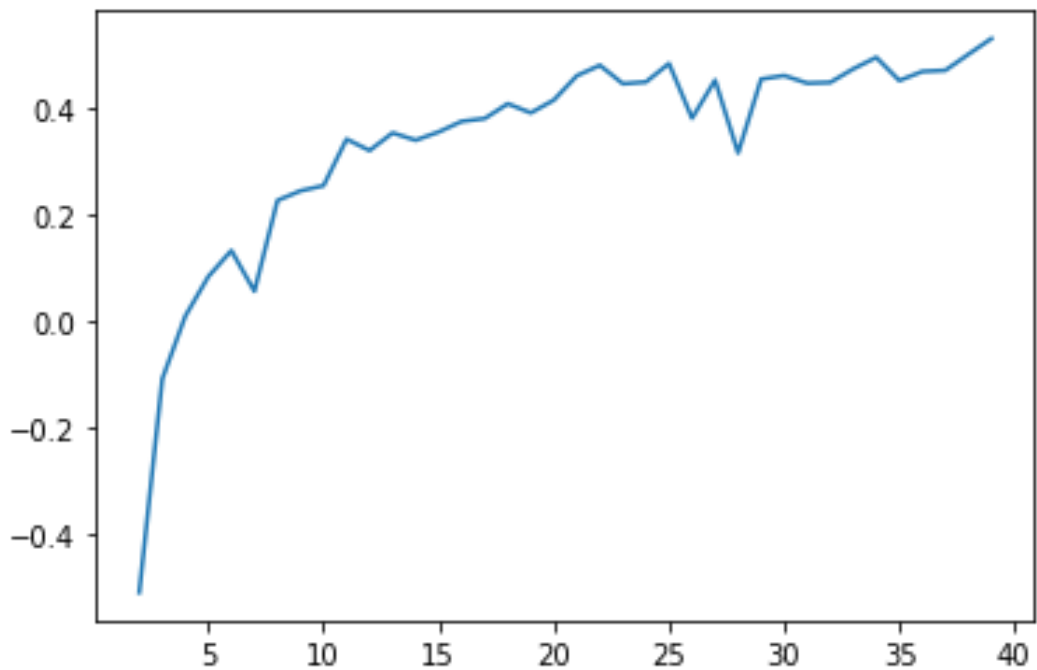


Рисунок 4.11 – Залежність зміни від приросту швидкості

Як і в інших роботах, ефективність запропонованої методики буде розглядатися на основі величини вектора, що розглядається. Це дослідження

працюватиме з 3 кластерами, зберігаючи постійний розмір вибірки на рівні 200 000, векторні розміри від 0 до 40.

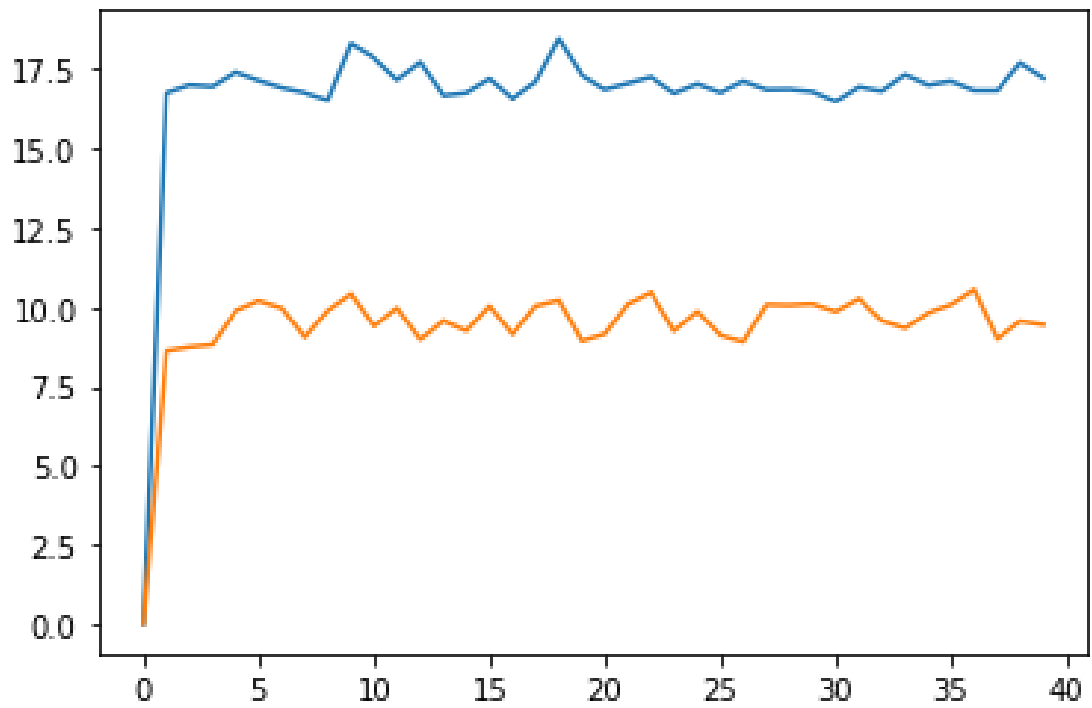


Рисунок 4.12 – Залежності від часу обрахунку від розмірності векторів

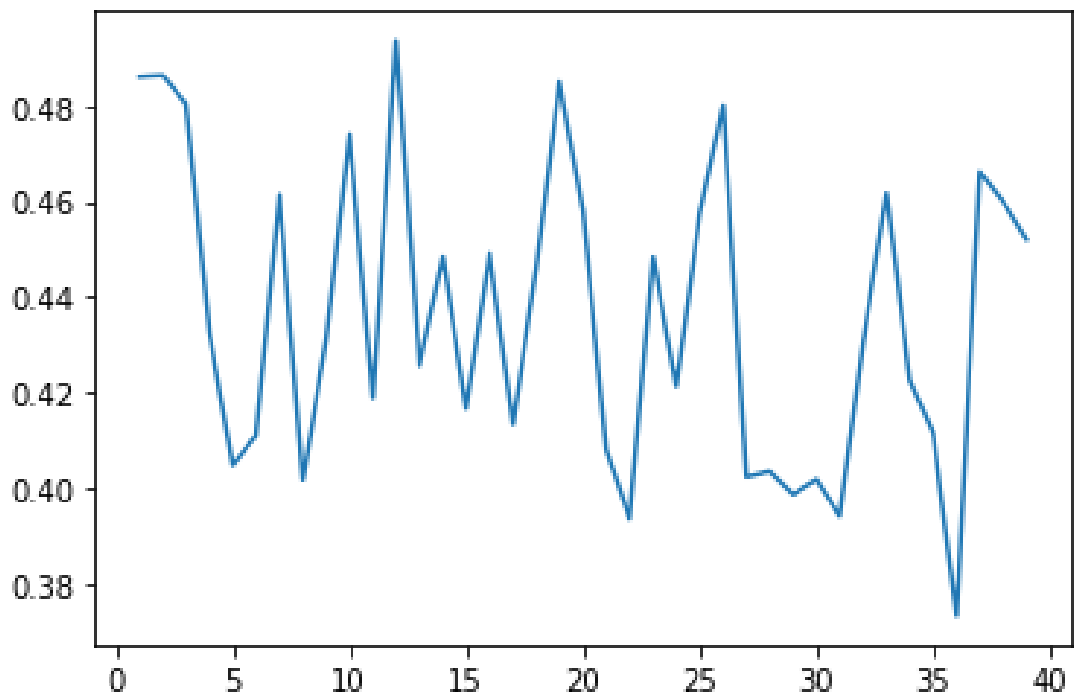


Рисунок 4.13 - Зміни відносного приросту швидкості

4.4 Синтезування регулятора для СККД

Враховуючи, що більша частина автоматизації та логіки належить контролеру, а допоміжне обладнання є приводом, вивчили різні варіанти механічного замку, серед яких електромеханічний підхід. Щоб уся система була безпечною та інтегрованою вздовж одного маршруту, вибір електромеханічної системи зробив механічний замок. Естафетний закон лідерства був задовільним для самосвідомості. Релейні засоби керування прості у впровадженні та мають найвищу ефективність, коли сигнал «ні» постійно подається назад до керуючої частини системи. Їх всього три: максимальний плюс, максимум мінус і нуль. Власне кажучи, релейні системи складні, тому що властивості їх компонентів складні в першу чергу. Таким чином, періоди часу, протягом яких закрита система і відкрита система працюють, не можуть бути попередньо розраховані; тобто вони не нав'язуються із зовнішнього світу, а визначаються внутрішніми властивостями системи. Визначено характерні особливості процесів регулювання в релейних системах. Вони можуть мати тривалий режим автоколивальності, а не лінійні осцилятори.

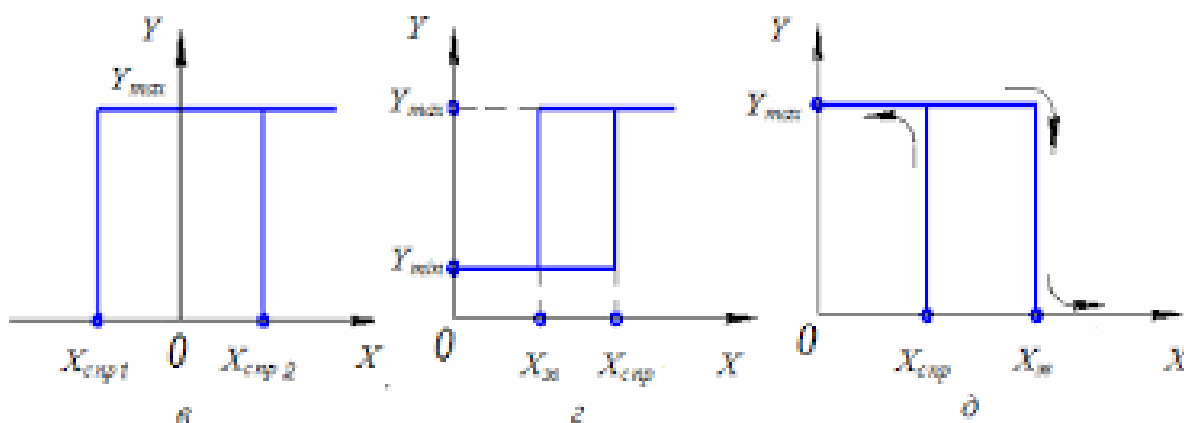


Рисунок 4.14 – Варіанти проходження сигналів

Якщо струми включення і вимикання реле не співпадають, з'являється петля гістерезису, яка вказує шлях виникнення автоколивального режиму. Щоб

усунути їх, накладається додатковий зворотний зв'язок, який залежить від швидкості двигуна. Статичну помилку, спричинену мертвою зоною реле, можна усунути, забезпечивши цю ідеальну характеристику реле. Звичайно, це неможливо зробити за допомогою мікроконтролера, який не контролює реле, що практично унеможлиблює це через затримку часу та помилку розрахунку.

4.5 Розробка DFD діаграми

По суті DFD близька до IDEF, оскільки також використовує принцип ієрархії та декомпіляції, але, на відміну від IDEF, є основним засобом моделювання функціональних вимог проєктованої системи. Метою створення такої діаграми є демонстрація того, як кожен процес перетворює свої вхідні дані на вихідні, а також виявити відносини між цими процесами. Ця діаграма зображує систему може «як буде». Перша діаграма з номером 0 називається контекстною і описує модельовану систему в загальному вигляді.

СКУД, крім здійснення автоматизованого пропускового режиму, надає, на мій погляд, не менш важливу для будь-якого підприємства функцію - обліку робочого часу співробітників за допомогою формування звітів. з одного боку, оператор СКУД – з іншого. Діаграма DFD0 представлена малюнку 4.15.

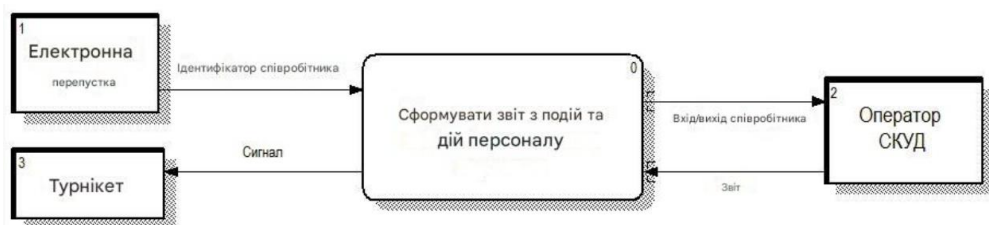


Рисунок 4.15 – DFD 0 діаграма

Далі виконується процес декомпозиції, що полягає у розбиття основного процесу на функціональні підсистеми з дотриманням принципу ієрархії. Щоб система змогла сформувати звіт, повинен відбутися наступний ланцюжок

подій: зчитування інформації з електронного пропуску співробітника, реєстрація події в системі (вхід/вихід або відмова) і після запиту на формування звіту відбувається безпосередньо сам процес формування звіту, отже, після декомпозиції діаграми DFD 0 ми отримаємо діаграму DFD 1, представлену на малюнку 4.16 і що складається з трьох підсистем.

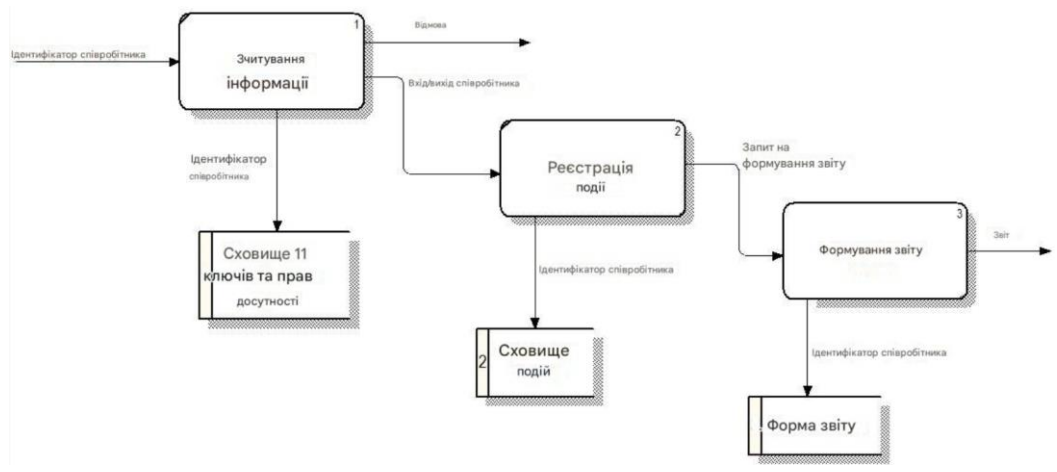


Рисунок 4.16 – DFD діаграма 1 рівня

Процес формування звіту декомпозуємо до DFD діаграми другого рівня, в якій покажемо, що для створення звіту необхідні критерії пошуку співробітників і зазначений період. Діаграма DFD 2 показано малюнку 4.17.

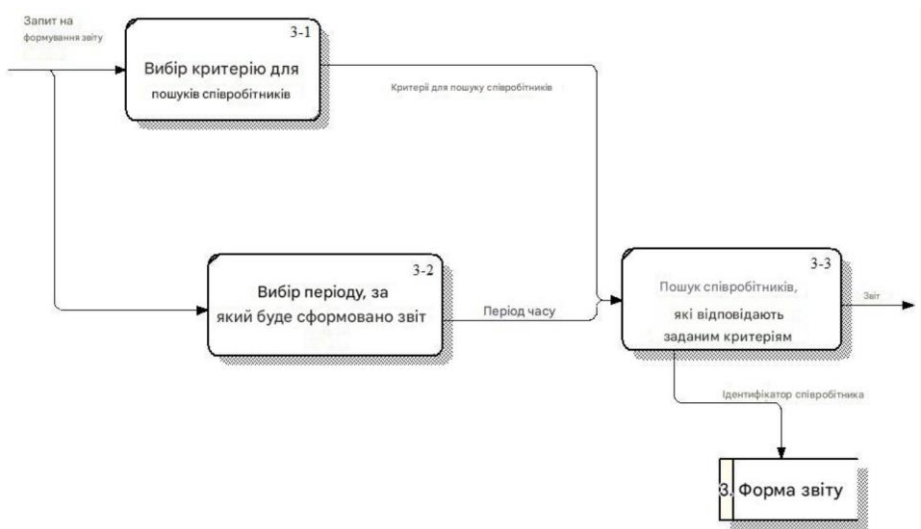


Рисунок 4.17 – DFD діаграма 2 рівня

4.6 Висновки до четвертого розділу

Таким чином, цей розділ ілюструє ефективність будь-якого оптимального алгоритму пошуку на наборі багатовимірних векторів. Запропоновано альтернативний оптимальний метод пошуку на основі векторної класифікації. Щоб отримати доступ до продуктивності цього підходу, було проведено 3 дослідження швидкості системи. Для спостереження ефектів змінювали довжину вектора, розмір вибірки та кількість кластерів.

Результати дослідження мали велике значення, оскільки вони довели, що обраний метод справді вплинув — це було відзначено приблизно в 30% регіонів із більш ніж 2-5 екземплярами розміру вибірки в базі даних, для якої він використовувався, тоді як з менше число, натомість пряме сортування мало більший ефект.

ВИСНОВКИ

Вона включала розгляд проблеми контролю доступу, сучасних шляхів вирішення цієї проблеми як однієї з робіт, а також конкретних методів розпізнавання осіб для подібних систем. Запропоновано елементи локальної системи автоматизації та побудовано функціональну схему автоматизації. Сучасні рішення в області розпізнавання обличчя зважають на швидкість дії з пропозицією оптимізувати пошук схожості за такими критеріями, як: Доступність Легкість впровадження

Таким чином, вся архітектура системи контролю доступу була вивчена в одному місці, включаючи базу даних, контролер і параксимальна модель автоматизації та машинного навчання.

У першому розділі показано, що в системі контролю та управління доступом немає нічого нового; напрямок уже визначено, але ще не остаточне вирішення проблеми захисту швидкості з точки зору контролю доступу. Оскільки швидкість спуску висока, тут використовуються підроблені картки чи мітки. Зі збільшенням рівня захисту починають помічати деякі проблеми з налаштуваннями системи, а особисті дані починають втрачати сьогодні в РК-телевізорах, які не забезпечують розпізнавання обличчя, навіть якщо доступ і безпека можуть бути завданнями, які вони виконують.

У другому розділі проведена розробка моделі автоматизації системи контролю та керування доступом. Наведено опис характеристик керування системою розпізнавання обличчя. Виконане обрання платформи для створення локальної системи автоматизації. Зроблено проектування застосунку, а також обрання бази даних. Запропонована монтажно-комутаційна схема автоматизації СККД.

У третьому розділі було розглянуто дослідження існуючих систем розпізнавання осіб, їх плюси і мінуси, дизайн і особливості додатків. Було проведено аналіз цього, щоб знайти найбільш відповідний дизайн для впровадження, що призвело до рішення використовувати FaceNet. У цьому розділі будуть детально описані всі частини цієї архітектури.

Четвертий розділ демонструє ефективність оптимального алгоритму пошуку на наборі багатовимірних векторів. Потім буде введено альтернативну оптимальну техніку пошуку на основі векторної категоризації. Було проведено три дослідження швидкості системи, щоб отримати доступ до продуктивності цього підходу. Були зроблені варіації довжини вектора, розміру вибірки та кількості кластерів, щоб спостерігати ефекти.

Отримані результати були дуже важливими, оскільки вони довели, що обраний метод щось дає – оцінено приблизно в 30% регіонів з більш ніж 2-5 екземплярами розміру вибірки в базі даних, для якої він використовувався, і замість того, щоб мати набагато більший ефект з менша кількістю, пряме сортування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. NEC. Facial Recognition [Електронний ресурс]. // Режим доступу: https://u.nec.com/solutions/security/technologies/face_recognition.html (дата звернення: 12.05.2018).
2. Neurotechnology. VeriLook SDK [Електронний ресурс]. // Режим доступу: <http://www.neurotechnology.com/> (дата звернення: 13.11.2024).
3. Techniques and Challenges of Face Recognition: A Critical Review [Електронний ресурс]. // Режим доступу: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (дата звернення: 13.11.2024).
4. TechniquesandChallengesof Face Recognition: A Critical Review [Електронний ресурс]. // Режим доступу: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (дата звернення: 13.11.2024).
5. AndreaF. Abate, Nappi Nappi, Riccio Riccio, Gabriele Sabatino 2D and 3D face recognition: A survey Pattern Recognition Letters, 28 (14) (2007), pp. 1885-1906
6. FaceNet: A Unified Embedding for Face Recognition and Clustering [Електронний ресурс]. // Режим доступу: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf (дата звернення: 13.11.2024).
7. Klein G., Murray D. Parallel tracking and mapping for small AR workspaces // Proc. of the 6th IEEE and ACM Intern. Symposium on Mixed and Augmented Reality (ISMAR 2007). Nara, Japan. 13-16 Nov., 2007. P. 225-234.
8. Mobile Robot Navigation. Edited by Alejandra Barrera. Published by InTech. Croatia. 2010.
9. Bischoff B., Nguyen-Tuong D., Streichert F., Ewert M., Knoll A.. Fusing Vision and Odometry for Accurate Indoor Robot Localization. II 12th

International Conference on Control, Automation, Robotics & Vision Guangzhou, China, 5-7th December 2012.

10. Chong K.S., Kleeman L. Accurate Odometry and Error Modelling for a Mobile Robot, MECSE-2006-6.

11. Навігація мобільних наземних роботів у недетермінованих середовищах. Сергієнко О.Ю., Карташов В.М., Колендовська М.М. Харків: ХНУРЕ, 2020. - 297 с.

12. Watanabe H., Dettloff W., Yount E. A VLSI Fuzzy Logic Inference Engine for Real-time Process Control // IEEE Journal of Solid State Circuits, 2000. – V.25, N.2. P.376 – 382.

13. Дубчак В. М. Вища математика в прикладах та задачах. Навчальний посібник / В.М.Дубчак, В.М.Пришляк, Л.І.Новицька. – Вінниця: ВНАУ, 2018. – 254 с

14. Харченко А.П. Вища математика в прикладах і задачах, частина І: Навчальний посібник / А.П.Харченко, В.О.Гаєвська, Г.В.Лисянська. – Х:НТМТ, 2017. – 194 с

15. Харченко А.П. Вища математика в прикладах і задачах, частина ІІ: Навчальний посібник / А.П.Харченко, В.О.Гаєвська, Г.В.Лисянська. – Х:НТМТ, 2017. – 233 с

16. Вища математика: базовий підручник для вузів / В.С.Пономаренка. – Х.: Фоліо, 2016. – 669 с

17. Герасимчук В. С. Вища математика. Повний курс у прикладах і задачах / В.С.Герасимчук, Г.С.Васильченко, В.І.Кравцов. – К.: Книги України ЛТД, 2015. – 470 с

18. Практикум з вищої математики: Навчальний посібник / За ред. В.О.Ковалю. – Ж: ЖДТУ, 2008. – 448 с

19. Вища математика. Загальний курс: Збірник задач та вправ. / А.Д.Тевяшев, О.Г.Литвин. URL: <https://www.twirpx.com/file/277182/> (дата звернення 12.05.2021)

20. Вища математика. Збірник задач: Навчальний посібник / В.П.Дубовик. URL: https://issuu.com/erudytnet/docs/1dubovik_v_p_yurik_i_i_vishcha_mate (дата звернення 12.11.2024)
21. Коруд В.І., Електротехніка: Підручник / В.І. Коруд, О.Є. Гамола, С.М. Малинівський; За заг. ред. В.І. Коруда. – 3-є вид., переробл. і доп. – Львів: Магнолія Плюс, 2006. – 447 с.
22. Михайленко В.Є., Інженерна та комп'ютерна графіка: Підручник / В.Є. Михайленко, В.В. Ванін, С.М. Ковальов; За ред. В.Є. Михайленка. – 6-е вид. – К.: Каравела, 2012. – 368 с.
23. Титаренко М.В., Електротехніка: Навчальний посібник/ М.В. Титаренко. – К.: Кондор, 2013. – 240 с.
24. Будіщев М. С. Електротехніка, електроніка та мікропроцесорна техніка : Підручник / М. С. Будіщев. – Львів : Афіша, 2001. – 424 с.
25. Колонтаєвський Ю. П. Промислова електроніка і мікросхемотехніка / Ю. П. Колонтаєвський, А. Г. Сосков. під ред. А. Г. Соскова. – Вид. 2-ге, виправл. і доповн. – Харків : ХДАМГ, 2003. – 281 с.
26. Теорія електропривода : Підручник / [М. Г. Попович, М.Г. Борисик, В.А. Гаврилюк та ін.] ; за ред. М. Г. Поповича. – Київ : Вища шк., 2003. – 454 с.
27. Руденко В. С. Промислова електроніка / В. С. Руденко, В. Я. Ромашко, В. В. Трифонюк. – Київ : Либідь, 2003. – 432 с.
28. Костін М. О. Теоретичні основи електротехніки [Текст]: підручник у 3 т. / М. О. Костін, О. Г. Шейкіна. – Дніпро: Вид-во ДНУЗТ, 2006. – Т. 1. – 336 с; 2007.- Т.2.- 276 с; 2011. – Т.3, Ч.1. – 224 с; 2012.– Т.3, Ч.2. – 352 с.
29. Качан Ю. Г. Лінійна електротехніка (теоретичні основи) [Текст]: навч. посібник / Ю. Г. Качан.– Запоріжжя: Вид-во Запорізької держ. інж. академії, 2005. – 206 с.

30. Гуржій А. М. Електротехніка та основи електроніки : підручник для здобувачів професійної (професійно-технічної) освіти / А. М. Гуржій, С. К. Мещанінов, А. Т. Нельга, В. М. Співак. - Київ : Літера ЛТД, 2020. - 288 с.
31. Електрика та магнетизм : підручник / Л. Д. Дідух. - Тернопіль : Підручники і посібники, 2020. - 464 с. - Режим доступу : <http://elartu.tntu.edu.ua/handle/lib/31412..>
32. Автоматика та електропривод техніки реєстрації інформації [Електронний ресурс] : навч. посіб. / Г. Г. Власюк, В. М. Співак, К. О. Трапезон, В. Б. Швайчен-ко. - Київ : Освіта України, 2010. - 159 с. - Режим доступу: <http://ela.kpi.ua/handle/123456789/19129>.
33. Колонтаєвський Ю. П. Електроніка і мікросхемотехніка : підручник / Ю. П. Колонтаєвський. - Київ : Каравела, 2006. - 384 с.
34. Макаренко В. В. Цифрова та імпульсна схемотехніка. Моделювання та аналіз : навч. посіб. для студентів, які навчаються за напрямом підготовки «Акустотехніка» [Електронний ресурс] / В. В. Макаренко, В. М. Співак ; НТУУ «КПІ». - Київ : НТУУ «КПІ», 2015. - 314 с. - Режим доступу: <https://ela.kpi.ua/handle/123456789/19099>.
35. Панчевний Б. І. Загальна електротехніка: теорія і практика / Б. І. Панчевний, Ю. Ф. Свергун. - 2-ге вид. - Київ : Каравела, 2004. - 440 с.
36. Воробйова О. М. Технічні засоби автоматизації: навч. посіб. / О. М. Воробйова, Ю. В. Флейта. - Одеса : ОНАЗ ім. О. С. Попова, 2018. - 208 с.
37. Бойко В. І. Мікрокомп'ютерна техніка / В. І. Бойко, А. Т. Нельга. - 2-ге вид. - Київ : Науково-методичний центр вищої освіти, 2008. - 254 с.
38. Електропривід сільськогосподарських машин, агрегатів та потокових ліній: Підручник / Є.Л. Жулай, Б.В. Зайцев, Ю.М. Лавріненко, О.С. Марченко, Д.Г. Войтюк; За ред. Є.Л. Жулая. – К.: Вища освіта, 2001. – 288 с.: іл.

39. Автоматизація технологічних процесів і системи автоматичного керування: Навчальний посібник /Барало О.В., Самойленко П.Г.,Гранат С.Є., Ковальов В.О. – К.: Аграрна освіта, 2010. – 557 с.
40. Експлуатація машин і обладнання: Навчальний посібник / Ружицький М.А., Рябець В.І., Кіяшко В.М. та ін. – К.: Аграрна освіта, 2010. – 617 с.
41. Матвійчук А. Я. Електротехніка: навчально-методичний посібник/ Матвійчук А. Я., В. Л. Стінянський; Вінницький державний педагогічний університет ім. М.Коцюбинського.– Вінниця, 2017. -270 с.
42. Загальна електротехніка з основами автоматики: Навчальний посібник / Т.В.Левченко. – К., 2010. – 358 с.
43. Технічний сервіс в агропромисловому комплексі: навчальний посібник / Коновалюк О.В., Кіяшко В.М., Колісник М.В. – К.: Аграрна освіта, 2013. – 404 с.
44. Електричні машини і апарати: навчальний посібник / Ю.М. Куценко,В.Ф. Яковлев та ін. – К.: Аграрна освіта, 2011. – 449 с.
45. Електроніка та мікросхемотехніка: Навчальний посібник / За ред. проф. В.Ф. Яковлева. – К.: Аграрна освіта, 2010. – 329 с.
46. Монтаж електрообладнання і систем керування / За заг. ред. проф. Яковлева В.Ф. – К.: Аграрна освіта, 2009. – 348 с.
47. Довідникова книга з електроенергетики: навчальний посібник/ П.В. Волох, М.П. Цоколенко, Л.В. Ревенко, В.А. Грічаненко та ін. –К. : Аграрна освіта, 2014. – 506 с.
48. Електроніка і мікропроцесорна техніка / Сенько В.І., Лисенко В.П., Юрченко О.М., Лукін В.Є., Руденський А.А. — К. : «Агроосвіта», 2015. — 676 с.
49. Електропостачання агропромислового комплексу :підруч. / Козирський В.В., Каплун В.В., Волошин С.М. – К. : Аграрна освіта, 2011. – 448 с.

50. Ремонт машин та обладнання : підручник / [Сідашенко О.І. та ін.]; за ред. проф. О.І. Сідашенка, О.А. Науменка. – К. : Агроосвіта, 2014. – 665 с.
51. Механізація, електрифікація та автоматизація сільськогосподарського виробництва : підруч. у 2 т : Т 1 / А.В. Рудь, І.М. Бендера, Д.Г. Войтюк та ін. ; за ред. А.В. Рудя. – К. : Агроосвіта, 2012. – 584 с.
52. Герасимчук І. До питання про впровадження нейро-лінгвістичного програмування у процес навчання іноземній мові у вищих військових навчальних закладах[Текст]/ І. Герасимчук//Вісник Львівського університету.-2003.-№1.-С. 39-44.
53. Субботин С.А. Синтез вейвлет-нейро-нечетких моделей для діагностики деталей авіадвигателів[Текст]/ С.А. Субботин//Вісник двигунобудування.-2006.-№2.-С. 163-168.
54. Лежнюк П.Д. Оптимальне керування нормальними режимами електроенергетичних систем критеріальним методом з використанням нейро-нечіткого моделювання[Текст]/ П.Д. Лежнюк, О.О. Рубаненко//Вісник Вінницького політехнічного інституту.-2012.-№1.-С. 127-131.
55. Арсенюк І. Р. Адаптивний алгоритм керування радіокерованим візком / І. Р. Арсенюк, В. І. Месюра, В. В. Савчук // Інтернет – Освіта – Наука – 2006 : збірник матеріалів V Міжнародної конференції. – Вінниця : УНІВЕРСУМ-Вінниця. – 2006. – Т. 2 . – С. 583 – 586.
56. Арсенюк І. Р. Розв’язання задачі подолання перешкод мобільним роботом / І. Р. Арсенюк, Д. А. Волхонський // Інформаційні технології та комп’ютерна інженерія. – 2006. – №2. – С. 67 – 72.
57. Арсенюк І. Р. Розпізнавання об’єктів у змінному середовищі / І. Р. Арсенюк, В. В. Колодний, Д. І. Будельков // Інтернет – Освіта – Наука –2006: збірник матеріалів V Міжнародної конференції. – Вінниця : УНІВЕРСУМ-Вінниця. – 2006. – Т. 2. – С. 603 – 605.

58. Арсенюк І. Р. Навчально-дослідницька система автоматичного керування радіокерованим візком / І. Р. Арсенюк, В. І. Месюра, Ю. Л. Ляшенко // Вісник Вінницького політехнічного інституту, 2010. – №1. – С. 112 – 115.

59. Корчиста О.В. Інтелектуальний модуль планування шляху мобільного робота / О.В Корчиста, В. І. Месюра // XLVI Науково-технічна конференція підрозділів Вінницького національного технічного університету (НТКП ВНТУ - 2017) / Електронне наукове видання матеріалів конференції. – Вінниця, 2017. – Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2026/1890>. // Вінниця:

60. Permana, S. D. H. Comparative Analysis of Pathfinding Algorithms A *, Dijkstra, and BFS on Maze Runner Game [Текст] / Silvester Dian Handy Permana, Ketut Bayu Yogha Bintoro, Budi Arifitama, Ade Syahputra // International Journal Of Information System & Technology. – 2018. – Vol. 1, №2. – Pp. 1–8.

61. Wengrow, J. A Common-Sense Guide to Data Structures and Algorithms [Текст] / J. Wengrow. – Pragmatic Bookshelf. – 2020. – 508 с. – ISBN 9781680607225.

62. Rohringer, W. Stochastic optimization of a cold atom experiment using a genetic algorithm Game [Текст] / W. Rohringer, R. Buckner, S. Manz, T. Betz, A. Perrin // Applied Physics Letters. – 2008. – Vol. 93, №26. – Pp. 93-116.

63. Sangdani, M. H. Genetic algorithm-based optimal computed torque control of a vision-based tracker robot: Simulation and experiment [Текст] / M. H. Sangdani, A. R. Tavalopour-Saleh // Engineering Applications of Artificial Intelligence. – 2018. – Vol. 67, №2. – Pp. 24-38.

64. Buckland, M. Programming game AI by example 1st Edition [Текст] / M. Buckland. – М. : Game AI. – 2004. – 495 с. – ISBN 978-1556220784.

65. Millington, I. Artificial Intelligence for Games [Текст] / I. Millington, J. Funge – М Artificial Intelligence for Games, 2006. – 845с.

66. Паласіос, Х. UNITY 5 Х. Програмування штучного інтелекту у іграх [Текст] / Х. Паласіос – М. : UNITY 5 Х, 2017. – 272 с. 26. Unity

Documentation [Электронный ресурс] – Режим доступа : [www/ URL: https://docs.unity3d.com/Manual/index.html/](http://www.unity3d.com/Manual/index.html) - 9.11.2020 г. – Загол. з екрану.

67. Алгоритми та методи [Электронный ресурс] – Режим доступа : [www/ URL: http://algolist.manual.ru](http://www.algolist.manual.ru) – 26.10.2020 г. – Загол. з екрану. 80

68. Needham, M. Graph Algorithms: Practical Examples in Apache Sparks and Neo4j [Текст] / M. Needham. - O'Reilly Media : Graph Algorithms, 2019. – 268 с. – ISBN 978-1492047681.

69. Choubey, N. S. A-Mazer with Genetic Algorithm [Текст] / N. S. Choubey // International Journal of Computer Applications. – 2018. – Vol. 58, №17. – Pp. 48-54. 42. Costa, A. A. A computational model for exploratory activity of rats with different anxiety levels in elevated plus-maze [Текст] / A. Costa, S. Morato, A. C. Roque, R. Tinos // Journal of Neuroscience Methods. – 2014. – Vol. 236, №1. – Pp. 44-50.

70. Vose, M. D. The Simple Genetic Algorithm: Foundations and Theory [Текст] / M. D. Vose. – The MIT Press. : Genetic Algorithm, 2009. – 220 с.

Додаток А

Стаття у фаховому журналі (подана до редакції журналу «Вимірювальна та обчислювальна техніка у технологічних процесах»)

УДК 004.93.1

DOI:

ФОРКУН Юрій
Хмельницький національний університет
<https://orcid.org/0000-0002-7906-4191>
forkynjv@khnu.km.ua
МАКАРИШКІН Денис
Хмельницький національний університет
<https://orcid.org/0000-0003-3447-811X>
makaryshkinde@khmnu.edu.ua
АНТОНЮК В.Р.
Хмельницький національний університет
ЛЮБЧИК Віталій
ТОВ «Карат»
vitaly1612@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ АВТОМАТИЗОВАНОГО КЕРУВАННЯ РЕЄСТРАЦІЄЮ ЛЮДЕЙ У ПРИМІЩЕННІ

В статті проведено дослідження методів реєстрації людей, що є основою систем контролю доступом. Дані системи призначені для персоналізації доступу у приміщення з обмеженим доступом. В основі цих систем полягає застосування комплексу взаємопов'язаного обладнання, що керує ідентифікацією контролем доступу у приміщення. Такі системи поділяються на автономні і мережеві. У статті розглянуті особливості кожного виду систем, їх переваги і недоліки.

Проаналізовано системи, що постачаються провідними світовими виробниками. Наведено основні особливості функціонування, переваги та недоліки. Розглянуто архітектури побудови програмних засобів контролю доступом. До них відносяться монолітні і мікросервісні архітектури. Описані особливості їх алгоритмів, переваги і недоліки. Наведено їх порівняння.

FORKUN Yuriy, MAKARYSHKIN Denys, ANTONYUK Vladyslav,
Khmelnitsky National University
LIUBCHYK Vitalii
Karat LTD

RESEARCH OF METHODS OF AUTOMATED MANAGEMENT OF REGISTRATION OF PEOPLE IN THE ROOM

The article studies the methods of registering people, which are the basis of access control systems. These systems are designed to personalize access to premises with limited access. The basis of these systems is the use of a complex of interconnected equipment that manages identification and access control to premises. Such systems are divided into autonomous and networked. The article examines the features of each type of system, their advantages and disadvantages.

Systems supplied by leading global manufacturers are analyzed. The main features of operation, advantages and disadvantages are presented. The architectures for building access control software tools are considered. These include monolithic and microservice architectures. The features of their algorithms, advantages and disadvantages are described. Their comparison is presented.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Завдання присвячене вирішенню прикладної проблеми, створенню системи управління доступом. Це, безумовно, має відношення до цього завдання, оскільки питання безпеки як в особистому, так і в державному секторі є перш за все, аналіз різноманітних систем цього типу, які діють на даний момент, має ряд особливостей їх застосування.

Перший з них – це опис описаних функцій, включаючи точність цих систем, простоту їх використання для користувача та здатність обробляти персональні дані. Оскільки ці три параметри мають найбільший зв'язок один з одним і безпосередньо впливають на кінцеву ефективність розробленої системи.

До цього моменту більшість компаній вже почали використовувати свої системи безпеки – СКУД (системи контролю та управління доступом). Зрештою, використання біометричних систем ідентифікації на підприємстві може призвести до значного підвищення безпеки компанії та її співробітників. У зв'язку зі стрімким зростанням вимог підприємств до систем біометричного розпізнавання найближчим часом очікується зростання інтересу до технологій розпізнавання осіб.

Аналіз останніх досліджень і публікацій

У 21 столітті постало питання організації захисту персональних даних і взагалі доступу до власності, важливих об'єктів і т.д. Ситуація стала дуже серйозною. Оскільки доступ до даних або об'єктів через неавторизованих осіб може призвести до жаклих результатів. У результаті було прийнято рішення про новий підхід до вирішення питань контролю доступу. Це рішення, яке пропонували люди вже досить давно. Були спроби застосувати різні варіанти, зокрема: коди доступу, які легко підробити, або отримати доступ до цієї інформації третьою стороною, магнітне зчитування стрічок або чіпів, але це рішення потребує зберігання особистої ідентифікаційної інформації, що призвело до низка питань щодо безпечного керування даними від імені користувача, контрольні картки, які мають непрямий характер, тощо. Як наслідок, тепер, коли загальна тенденція до використання обличчя як засобу ідентифікації почала поширюватися, за належного підходу до цього типу контролю та управління доступом його можна вважати найефективнішим рішенням для захисту людей. [1]

Система контролю та управління доступом (СКУД) – це сукупність програмно-апаратних засобів, яка призначена для обмеження доступу до об'єкта та реєстрації використовуваних точок доступу. Основним завданням контролю та управління доступом до конкретної території (об'єкта) є:

- контроль та обмеження доступу на конкретну територію - це дає змогу визначити чіткі правила для певної групи осіб щодо часу доступу та ступеня доступу, ці правила можна використовувати для визначення відповідальності та надання конкретних деталей щодо об'єкт з підвищеною безпекою.

- ідентифікація того, хто має доступ до певної території – ця інформація важлива, оскільки дозволяє відслідковувати як час роботи, так і проблеми, що виникають. [1]

Додаткові обов'язки:

Облік відпрацьованого часу;

Управління базою даних персоналу та відвідувачів також входить до цієї категорії.

- інтеграція з системою безпеки, приклад:

- з системою відеоспостереження, яка об'єднує системні події, які вже заархівовані, надсилаючи в систему сповіщення про необхідність початку запису та повертаючи камеру на фіксацію наслідків зафіксованої підозрілої події;

- із системою охоронної сигналізації (СОС) це дозволяє отримати доступ до зон обмеженого доступу або зон, які автоматично поставлені під охорону.

- із системою пожежної сигналізації (СПС), яка отримує інформацію про стан пожежних сповіщувачів, автоматичне розмикання евакуаційних дверей і закриття дверей у разі пожежної тривоги. [1]

Формулювання цілей статті

У зв'язку з цим була поставлена мета даної статті – провести аналіз методів та засобів автоматизованого керування реєстрацією людей у приміщенні на основі розпізнавання осіб.

Виклад основного матеріалу

У цій спробі пропонується використовувати підхід до керування даними та контролю доступу за допомогою використання технології розпізнавання обличчя. Перевага цього підходу полягає в тому, що він зменшує потребу в особистих даних, водночас забезпечуючи користувачеві максимальну легкість і відповідний поріг ефективності.

СККД поділяють на два типи - мережеві та автономні.

Мережеві РК-дисплеї мають атрибут, що кожен об'єкт управління доступом (контролер) пов'язаний із сервером. Тобто він містить принаймні два компоненти: локальну систему автоматизації (виконавчий механізм, пристрій зчитування та пристрій обмеження доступу) і серверну частину, яка обробляє запити на доступ від локальної системи автоматизації (клієнт). Такий стиль СККД вигідний для великих об'єктів, оскільки регулювати навіть десяток автономних дверей стає вкрай складно. Використовувати мережеві СККД корисно в таких ситуаціях:

Коли це непрактично або рекомендовано встановити комплексну внутрішню систему автоматизації.

Якщо систему можна розділити на кілька частин і скопіювати в інші системи (наприклад, пристрій з обмеженим доступом), тоді потрібно буде встановити більше обладнання для обробки та зберігання даних, що матиме негативний вплив на підтримку та витрати система.

Коли локальні дані не потрібні, а продуктивність системи невисока, саме час перейти до хмар. в особистих приміщеннях тощо.

Системи контролю доступу до мережі мають значну перевагу, яка полягає в здатності поширювати та диференціювати системи контролю доступу, роблячи їх автономними, легко розширюваними та керованими. Бездротові технології (радіоканали) можна використовувати в системах контролю доступу до мережі. Використання бездротових мереж, як правило, визначається конкретними ситуаціями: важко або неможливо підключити дротовий зв'язок до об'єктів, це збільшує фінансові витрати на встановлення точки доступу. Для радіостанцій доступно багато опцій, але лише деякі з них реально використовуються в системі SKKD.

Bluetooth. Цей тип бездротового пристрою передачі даних схожий на Ethernet щодо аналогового. Його властивість полягає в тому, що немає необхідності використовувати паралельні комунікації для підключення компонентів при використанні протоколу RS-485. Однак це рішення не є ідеальним для великих класів об'єктів через обмежений діапазон і проблеми безпеки, пов'язані з технологією Wi-Fi. Ці проблеми роблять його непридатним для великих установок, відстань до приймача (комп'ютера, який оброблятиме дані), ймовірно, буде виправлено, і проблеми необхідності підключення до іншого користувача буде уникнуто. Це рішення більше підходить для локальної домашньої автоматизації, яка матиме одного користувача та обмежену відстань до приймача. Однак цей тип об'єднання є дуже енергоефективним, що може бути корисним у ситуаціях, коли система переходить у режим очікування для генерування електроенергії.

Wi-Fi. Основною перевагою цієї радіочастоти є велика відстань зв'язку, яка може досягати кількох сотень метрів. Це особливо важливо для з'єднання об'єктів, які знаходяться далеко. Крім того, зменшуються тимчасові та фінансові витрати, пов'язані з прокладанням комунікацій. Крім того, цей тип зв'язку має вищий ступінь безпеки, пов'язаний із переданими пакетами. При правильній конфігурації цього типу підключення ми можемо гарантувати, що пакети досягнуть сервера та користувача, обидва вони мають вирішальне значення для належної роботи автоматизації.

Автономні системи дешевші, простіші в експлуатації, не вимагають прокладання сотень метрів кабелю, додаткових пристроїв, які підключаються до сервера, або самого сервера. І навпаки, негативні аспекти цих типів систем включають неможливість створювати звіти, відсутність інформації про робочий час, відсутність контролю над подіями та неможливість дистанційного керування. Вище були описані різні типи системи цього типу, одна з найбільш істотних небезпек - це неможливість запам'ятати пароль, який описаний вище. Крім того,

такі типи систем мають широкі обмеження щодо застосування. Однак навіть цей тип системи має переваги, окрім згаданої вище здатності продовжувати функціонування, коли один із критичних компонентів системи вимкнено, система також стійка до збоїв через втрату зв'язку з сервером, на відміну від мережі. ССКД де втрата зв'язку з сервером призводить до нездатності всієї системи функціонувати, у цьому типі ССКД такої проблеми немає. При виборі автономної системи з високими вимогами безпеки важливо врахувати наступне:

- зчитувач повинен бути ізольований від контролера, щоб зовнішні дроти, через які можна відкрити замок, були недоступні.
- контролер повинен мати джерело живлення, якщо зовнішнє джерело живлення виходить з ладу.

У рамках системи автономного доступу також використовуються електронні замки, які передають інформацію по бездротових каналах: у дверях розташований механічний замок з електронним управлінням і вбудованим зчитувальним пристроєм. Замок пов'язаний з концентратором через радіочастотний канал, це вже передає інформацію по дроту на робочу станцію, на якій встановлено програмне забезпечення.

З кожним роком кількість людей, які цікавляться технологіями розпізнавання осіб, значно збільшується. Сьогодні в різних сферах людської діяльності використовується кілька десятків систем розпізнавання.

Лідуючими компаніями з розробки таких систем є: NEC Corporation (Японія), Cognitec Systems GMBH (Німеччина), Neurotechnology (Литва).

Система «FaceVACS-VideoScan»

«FaceVACS-VideoScan» — це просте у використанні настроюване програмне забезпечення для розпізнавання обличчя у реальному часі, створене компанією Cognitec Systems.

За роботу системи «FaceVACS-Video» відповідає системний компонент під назвою FaceVACS-VideoScan.

- сервер відеопотоку, який керує потоком відео;
- сервер відеоспостереження координує всі компоненти системи та виконує основні біологічні операції.
- обчислювальний вузол, призначений для обчислення розподілу обчислювальних навантажень.

Інтерфейс користувача:

- диспетчер сигналів, який приймає сповіщення про події та керує мобільними пристроями, оперативною базою даних та набором інтеграторів.

До цього моменту технологія FaceVACS використовувала алгоритм B10T9 для розпізнавання обличчя. Цей алгоритм стійкий до змін виразу обличчя, повороту обличчя ($\pm 15^\circ$), часткового закриття, використання сонцезахисних окулярів і змін освітлення.

Крім того, система FaceVACS має додаткові можливості:

- можливість стежити за кількома людьми одночасно;
- порівняння індивідів ведеться в режимі реального часу.
- здатність показувати та передавати статистичні дані про потоки.
- підтримка інтерактивної реєстрації власності;
- використання C++'s API і Web Services' API.

Система "NEC's Face Recognition" компанії "NEC"

Система розпізнавання обличчя у NEC є однією з найдосконаліших у японській країні, ця система розроблена компанією NEC і розпізнає людей із фільмів десятирічної давнини, навіть якщо людина в окулярах або стоїть обличчям. Усі розпізані обличчя зберігаються в базі даних, тому, якщо вам потрібно отримати доступ до всієї історії реєстрації відео, ви можете просто відкрити реєстраційну інформацію та переглянути дату й час будь-якого раніше збереженого зображення.

Технологія, відома як NEC, перевершує інші системи розпізнавання як за швидкістю, так і за точністю. Це ефективно в різних сценаріях, у тому числі при роботі з відео низької якості та сильно стисненими зображеннями. NEC оцінює індивідуальні характеристики людини (розмір, форму зиниць, лінії носа та рота та

їх розташування відносно інших осіб у базі даних), а потім знаходить схожу особу в базі даних на основі цієї інформації.

Система містить декілька модулів, які реалізують наступні алгоритми:

1. Використовується метод узагальненого узгодження (GMFD), який має високу швидкість виявлення та високу точність розпізнавання облич. Метод GMFD складається з нейронних мереж, які спочатку шукають пари очей.

2. Алгоритм PSM (Perturbation Space Method) допомагає вам вирішити проблеми, пов'язані з визначенням місця розташування людини в кадрі (хтось під кутом або просто за межами кадру).

3. Метод ARBM (Adaptive Regional Blend Matching) зменшує вплив незначних змін обличчя (наприклад, зміни виразу обличчя, наявність окулярів або головного убору) на точність розпізнавання [2].

Система розпізнавання обличчя NeoFace має наступні атрибути:

- Можливість спостерігати та регулювати в реальному часі.
- індивідуальна ідентифікація;
- Багаторазове підтвердження;
- Можливість пошуку подій у базі даних;
- Наявність журналу записаних зображень осіб.
- Відкритість для нових напрямків руху до 45 градусів від попереднього положення;
- Елемент керування «перетягуванням»;
- Велика ємність і необмежений розмір бази даних;
- Незалежно від напрямку погляду та особливостей обличчя (окуляри, борода та виразні рухи обличчя).

Система VeriLook SDK компанії Neurotechnology

VeriLook SDK — система ідентифікації людини, створена компанією Neurotechnology. Це система, яка розпізнає людей за присутністю в кадрі та швидко їх ідентифікує (знаходить до 100 тис. осіб за секунду). VeriLook SDK доступний як повна платформа розробки програмного забезпечення та підтримує різноманітні пристрої на Windows, Linux, Mac OS X, iOS та Android.

Алгоритм VeriLook використовує технологію цифрової обробки зображень на основі глибоких нейронних мереж для локалізації людини.

Основними перевагами системи VeriLook є відсутність необхідності взаємодіяти з пристроями, які сканують обличчя, і швидке впровадження біометричних функцій, які ідентифікують людей, у програмах клієнтів. Крім того, є кілька інших переваг:

- Одночасна обробка кількох осіб.
- Класифікація за статтю. Стать можна позначити для кожної особи на портреті.
- Розпізнавання облич у реальному часі. VeriLook визначає, чи людина на відео насправді жива чи це фотографія.
- Розпізнавання емоцій. VeriLook розглядає шість основних емоцій: гнів, відраза, страх, щастя, сум і здивування;
- Особистісні характеристики. VeriLook можна налаштувати для розпізнавання певних атрибутів під час збору обличчя - усмішка, відкритий рот, закриті очі, окуляри, борода чи вуса;
- Визначення краси зовнішнього вигляду обличчя. Поріг якості можна використовувати під час реєстрації фізичних осіб, щоб гарантувати, що в базі даних зберігаються лише найбільш кваліфіковані шаблони.
- Кілька прикладів однієї особи. Ці зразки можна оцінювати з різних точок зору та в різний час, що сприяє підвищенню якості порівняння.
- Здатність розпізнавати. Параметри VeriLook також доступні для порівняння 1 до 1 (перевірка), а також у режимі багаторазового порівняння.
- Маленький дизайн обличчя. Шаблон особи може мати розмір 4 байти;

- Переваги загального режиму. Цей метод створює різноманітні узагальнені атрибути обличчя з кількох зображень самого об'єкта.

Алгоритм VeriLook здатний розпізнавати межі, які спостерігалися в інфрачервоному спектрі.

Основні елементи СККД.

Ці методи досить різноманітні, включаючи турнікети, двері з електромагнітним ключем тощо.

- Електромагнітні замки - більшість із них вимикаються, коли до них подається живлення, тому вони популярні для використання на шляхах евакуації при пожежі.

- Турнікети - механізм перемикання між поворотним і ковзним рухом за допомогою штифтів, які запобігають руху. Він може не прикривати, а лише сповільнювати швидкість руху при необхідності.

Якщо процес верифікації користувача ще можливий.

- Електромеханічні замки – вони досить стійкі до злому (якщо замок механічно потужний), вони також мають механічне скидання (це означає, що якщо ви натиснете на замок, він буде відчинено, доки ви не відчините двері).

- Шлюзові кабінки: вони працюють у банках, у режимних установах (у компаніях, які мають підвищену стурбованість безпекою).

- Ворота та шлагбауми - в основному, вони розташовуються на в'їздах на територію компанії, на автостоянках і паркінгах, на під'їздах до господарських будівель, у дворах житлових будинків. Основною вимогою є здатність витримувати кліматичні умови та можливість автоматизації (через систему контролю доступу). При проектуванні організації контролю доступу до системи пред'являються додаткові вимоги - додаткові можливості включають можливість зчитування табличок, розмір яких перевищує термін експлуатації, розпізнавання номерів автомобілів (при поєднанні з системою відеоспостереження).

Найпоширеніші види виконання - це карта, брелок, ярлик. Є основним компонентом системи контролю доступу, який зберігає код, який використовується для визначення прав власника («ідентифікація»). Це може бути картка пам'яті Touch, безконтактна картка (наприклад, RFID) або картка з магнітною смугою. Код, який вводиться з клавіатури, також може служити відмінністю. Сьогодні їх не дуже складно поспувати. Зіставляється з біометричними показниками, якими є: відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення людини, малюнок капілярних ліній на долоні.

Надійність (стійкість до підробок) системи контролю доступу в першу чергу залежить від типу використовуваного ідентифікатора: найпоширеніші безконтактні картки підробляються на обладнанні, яке легко визначити. Як наслідок, ці ідентифікатори не підходять для об'єктів, які потребують більш широкого захисту. Більш фундаментальна відмінність у безпеці полягає в тому, що RFID забезпечують вищий рівень безпеки, код картки зберігається в захищеній зоні та зашифрований. Однак цей метод все ще не є надійним, оскільки не потрібно розшифровувати мітку, а ви можете лише відтворити її зашифроване значення на іншій платформі. Зрештою, більш точним методом, як було сказано раніше, є біометричний показник. Не всі біометричні показники легко зчитуються, тому необхідно використовувати такий, який не потребує додаткового обладнання, окрім простої камери або іншого пристрою для зчитування інформації та отримання інформації за короткий проміжок часу. Це риси сітківки ока, підпис обличчя на фотографії. Однак це ставить питання щодо збереження даних, оскільки це особиста інформація, відмінна від обличчя, і може бути використана в іншій системі. Сьогодні навіть у мобільних телефонах є зчитувач відбитків пальців, ця інформація важлива, тому підробляти її не варто. На відміну від обличчя, дані надзвичайно важко підробити за допомогою тривимірної карти тегів, тому що для цього потрібно буде використовувати обладнання, а використання простої фотокартки унеможливить доступ до системи. без обличчя. Крім того, зчитувач у системі використовує подібну технологію, і використання простої фотокартки призведе до неможливості надати доступ без обличчя.

Це є невід'ємною частиною системи: контролер визначає, чи дозволено власнику ідентифікатора проходити через точку доступу, система зберігає коди для прав доступу ідентифікатора в списку, а контролер

визначає, чи має власник права. Коли людина зчитує (подає читачеві) код, відбувається порівняння між ними, і на основі результатів порівняння приймається рішення. Для роботи контролера потрібне живлення, тому контролери зазвичай мають окрему батарею, яка підтримує його роботу протягом кількох годин або днів у разі збою живлення. Однак у дуже складних системах контролер частіше бере участь у процесі керування без фактичної обробки даних, він приймає рішення на основі результатів сервера, які можуть бути отримані після обробки певного набору даних. Контролер є центральною частиною локальної системи автоматизації, він обробляє сигнали датчиків і передає команди виконавчим механізмам.

Це пристрій, який отримує ідентифікаційний код і передає його на контролер. Варіанти зчитувача залежать від типу ідентифікатора: для «планшета», який складається з двох електричних компонентів (один є «кишеньковим»), для картки, яка складається з електронної плати та антени, у цьому випадку читач повинен вставити телевізійну камеру в зображення. Якщо зчитувач розміщений на дорозі (ворота, зовнішній в'їзд у будівлю та під'їзд до стоянки), то він повинен витримувати кліматичне навантаження перепадів температур, опадів, а особливо, якщо місцевість має суворий клімат, то читач має вміти це витримати. Якщо існує ризик руйнування, важлива також механічна потужність (сталевий корпус). Окремо можна вибрати зчитувачі, які ідентифікують об'єкти на відстані до 50 м. Ці типи систем корисні на шосе, автострадах і в'їздах до блокпостів. Зчитувачі, ідентифіковані як такі, зазвичай мають активну мітку (містять вбудований акумулятор). Для відбитків рук або пальців це ультразвукові датчики, які створюють чітке зображення (відбиток) відповідного методу авторизації. У цих методах зображення характеризується специфічними та вимогливими вимогами, що вимагає використання ультразвукових датчиків для створення відбитка. У випадках, коли використовується обличчя, необхідна камера глибини як засіб перевірки.

Після вивчення існуючих рішень і підходів були визначені вимоги, які б відповідали даним умовам. Щоб система була застосована, мають бути виконані наступні передумови.

- Можливість зв'язку з усіма периферійними пристроями через одну універсальну точку доступу;
- Швидкість системи;
- Здатність до збільшення;
- Можливість зберігати та додавати інформацію про нових та існуючих користувачів;
- Можливість перепроєктувати систему без переривання її функціонування;
- Масштабність системи як у вертикальному, так і в горизонтальному напрямках;
- Стабільність системи.

Після того, як всі вимоги були виконані, ми мали можливість спостерігати всю проблему та вибрати підходи до її вирішення.

Як компонент системи контролю та управління доступом, наявність руху документується дискретним датчиком руху; фото зображення. Вплив керування - це сигнал, який посилає контролер після обробки фотографії через модель, цей сигнал потім передається у вигляді двійкового числа на вихід. У нашому прикладі живлення є, але воно не надсилається на плату керування приводу.

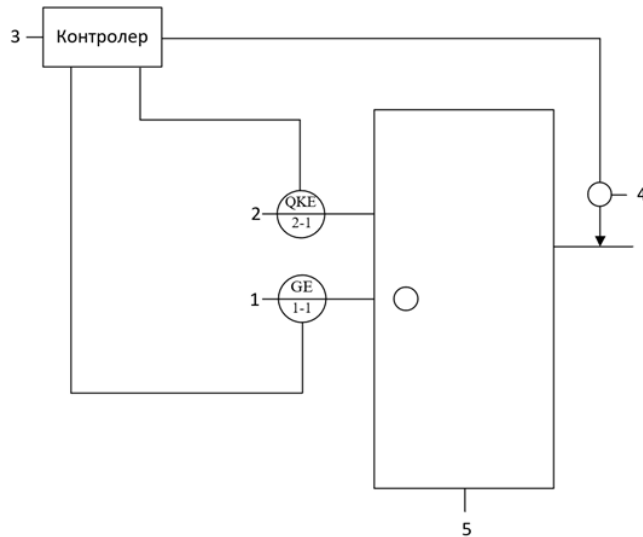


Рис. 1. Функціональна схема керування СККД

На функціональній схемі СККД (рис. 1.) зображено 5 основних компонентів системи:

1. Датчик руху, який являє собою інфрачервоний випромінювач і приймач.
2. Камера, яка документує зображення.
3. Контролер повинен взаємодіяти з системою.
4. Механізм замкнення.
5. Пристрій блокування фізичного доступу.

Система працює за такими принципами: людина, яка бажає увійти в приміщення, наближається до наявного фізичного бар'єру, спрацьовує датчик руху та надходить сигнал на контролер. Контролер інтерпретує цей сигнал і наказує камері зробити знімок. Камера зробить знімок і поверне його до контролера, який потім обробить фотографію за допомогою моделі. Після отримання результату (% подібності) контролер визначає, чи слід надати чи заборонити доступ, якщо вони це зроблять, вони надішлють сигнал виконавчому механізму (виконавчий механізм зазвичай закритий).

Зараз використовується багато різних шаблонів архітектури програмного забезпечення. Давайте розглянемо три, які можуть допомогти у вирішенні нашої проблеми:

конструкція «моноліт».

- Дизайн «Малі послуги».

- Дизайн «Клієнт-сервер».

Обговоримо кожен із цих підходів докладніше.

Монолітна архітектура — це традиційний дизайн програмного забезпечення, що складається з одного модуля, який функціонує автономно та незалежно від інших програм. Моноліт часто характеризують як великий і неінтуїтивно зрозумілий, ці два слова добре описують загальну архітектуру розробки програмного забезпечення.

Монолітна архітектура - це окрема велика мережа, яка має єдиний базовий код і використовується для об'єднання всіх бізнес-завдань. Щоб внести зміни в цю програму, ви повинні спочатку оновити весь стек через кодову базу, а потім випустити та розгорнути оновлену версію сервіс-орієнтованого інтерфейсу. Це виключає можливість робити оновлення та займає багато часу.

Моноліти корисно використовувати на ранніх стадіях проектів, щоб полегшити розгортання коду без необхідності витрачати надто багато розумової енергії на підтримку коду. Це полегшує негайний випуск усього в монолітній програмі.

Рисунок 2 ілюструє схему монолітної конструкції. Це демонструє, що всі складові компоненти включені в одну програмну програму. Тобто все виконується одним механізмом, який знаходиться в одному місці як єдина служба.

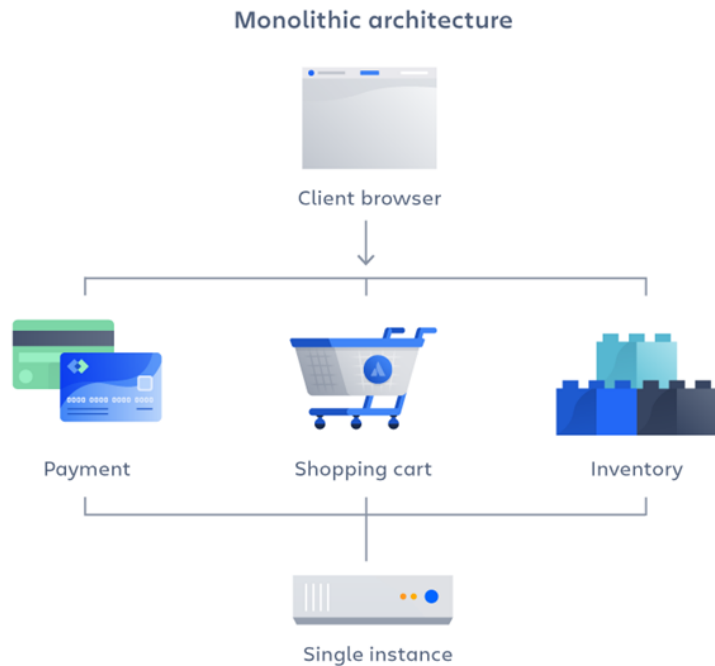


Рис. 2. Схематичне зображення монолітної архітектури

Переваги цієї конструкції:

- Легкий монтаж. Використання одного виконуваного файлу або каталогу спрощує розгортання. розвиток. Простіше створити програму, якщо вона створена з єдиним базовим кодом.
- Продуктивність. У централізованій базі коду та сховищі один API часто може служити інтерфейсом для кількох мікросервісів.
- Скорочене тестування. Монолітна програма — це єдиний централізований компонент, який забезпечує швидше тестування всієї системи, ніж розподілена програма.
- Легке усунення несправностей. Весь код знаходиться в одному місці, що полегшує виконання запитів і виявлення проблем.

Недоліки такої конструкції:

- Зниження швидкості росту. Велика надійна програма, яка є складною та уповільнює процес розробки, є великою.
- Масштабованість. Окремі компоненти не можуть бути змінені.
- Міцність. Збій в одному з модулів може негативно вплинути на доступність програми.
- Недостатня гнучкість. Можливості цілісних програм обмежені застосовуваними технологіями.
- Перешкоди для впровадження технологій. Будь-які зміни в інфраструктурі чи мові програмування вплинуть на всю програму, що зазвичай вимагає збільшення витрат і часу.
- Реалізація. Внесення незначних змін вимагатиме перетворення всієї монолітної програми.

Наступний тип архітектурної реалізації - "Мікросервіси". Архітектура мікросервісів (або просто «мікросервіси») — це стиль архітектури, який базується на незалежному виконанні кількох сервісів. Ці служби мають власну логіку та базу даних, призначену для конкретної мети. Розгортання, тестування та масштабування є внутрішніми для кожної служби. Мікросервіси розкладають великі бізнес-завдання на численні індивідуальні бази коду. Мікросервіси не зменшують складність, але вони роблять будь-яку складність очевидною та більш керованою, розбиваючи завдання на менші процеси, які не залежать один від одного та сприяють ширшій картині. На малюнку 3. показано склад компонентів цієї архітектури.

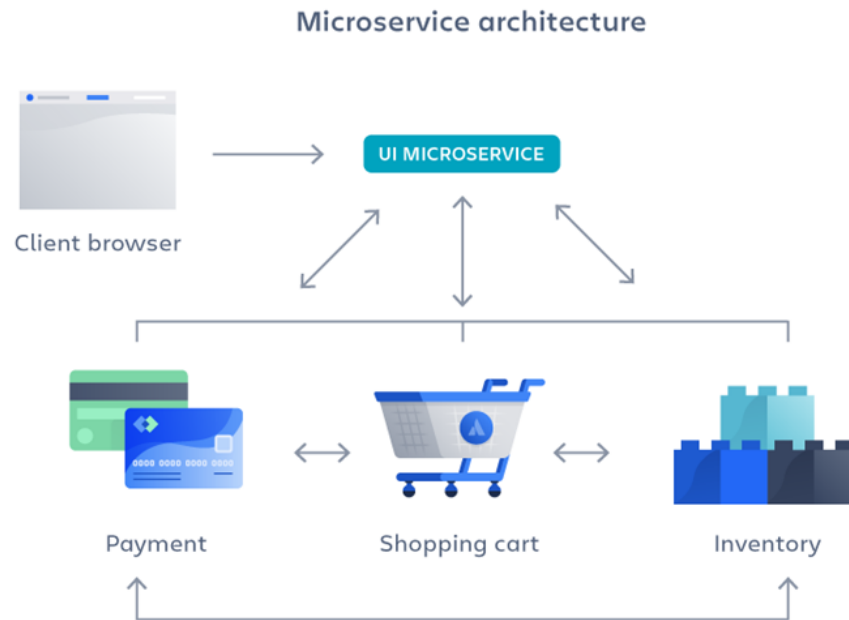


Рис. 3. Діаграма “Мікросервісної” архітектури

Опишемо наступний тип архітектурного натхнення - "Мікросервіси". Архітектура мікросервісів (або просто «мікросервіси») — це стиль архітектури, який базується на незалежному виконанні кількох сервісів. Ці служби мають власну логіку та базу даних, призначену для конкретної мети. Розгортання, тестування та масштабування є внутрішніми для кожної служби. Мікросервіси розкладають великі бізнес-завдання на численні індивідуальні бази коду. Мікросервіси не зменшують складність, але вони роблять будь-яку складність очевидною та більш керованою, розбиваючи завдання на менші процеси, які не залежать один від одного та сприяють ширшій картині. На малюнку 3. показано склад компонентів цієї архітектури.

- Простота обслуговування та тестування. Команди можуть вивчати нові функції та повертатися до попередньої версії, якщо щось неефективне. Це зменшує складність оновлень коду та прискорює випуск нових функцій для громадськості. Крім того, легко знаходити та виправляти помилки та проблеми в окремих службах.

- Розгортання, яке не залежить від хоста. Мікросервіси розглядаються як окремі компоненти, що дозволяє легко і швидко реалізувати окремий розподіл окремих функцій.

- Гнучкість технологій. Використовуючи дизайн мікросервісів, команди мають можливість використовувати інструменти на основі своїх уподобань.

- Висока надійність. Вносячи зміни в певний сервіс, можна не побоюватися, що програма вийде з ладу.

Переваги цього варіанту:

- Збільшення розвитку зростання. Мікросервіси ускладнюють монолітну архітектуру порівняно з іншими проектами, оскільки існує більше сервісів, створених кількома командами в різних місцях. Якщо ріст не регулюється належним чином, це сповільнить розвиток і знизить ефективність роботи.

- Зростання вартості інфраструктури. Кожен новий мікросервіс може мати власні витрати, пов'язані з набором тестів, інструкціями щодо розгортання програмного забезпечення, інфраструктурою для розміщення програмного забезпечення, інструментами для моніторингу програмного забезпечення тощо.

- Додаткові витрати, пов'язані з організацією. Команди потребують додаткового спілкування та співпраці, щоб полегшити оновлення та взаємодію.

- Проблеми з налагодженням. Кожен мікросервіс має власний набір журналів, що ускладнює усунення неполадок. Крім того, можуть виникнути додаткові ускладнення, якщо одна бізнес-процедура виконується на кількох машинах.

- Відсутність стандартизації. Без спільної платформи може виникнути ситуація, коли перелік мов, стандартів для ведення журналів та інструментів для моніторингу збільшиться.

- Відсутні запити щодо власності майнових питань. У міру створення нових послуг збільшується кількість команд, які в них беруть участь. Зрештою, важче визначити, які послуги може надати команда та до кого слід звертатися по допомогу.

Розглянемо останню зі списку з наведених архітектур - "Клієнт - серверна". "Клієнт - сервер" - поняття що об'єднує в собі два окремих шарів, а саме:

- Клієнт - це локальний комп'ютер (або інший пристрій з обчислювальними можливостями), який діє як віртуальний користувач, цей пристрій запитує дані або певну групу дій від сервера.

- Сервер: потужний комп'ютер або спеціальне системне обладнання, яке призначене для виконання конкретного завдання під час виконання комп'ютерних програм. Він виконує роботу з обслуговування за запитами клієнтів, надає користувачам доступ до певних ресурсів системи, зберігає інформацію або працює з базою даних.

Атрибути цієї моделі полягають у тому, що користувач запитує певну дію від сервера, яка обробляється автоматично, а кінцевий результат надсилається клієнту. Сервер здатний обслуговувати декілька клієнтів одночасно.

Якщо одночасно надходить більше ніж один запит, ці запити поміщаються в окрему чергу, і сервер виконуватиме їх у порядку. Іноді запити мають свої пріоритети. Деякі більш важливі запити завжди виконуватимуться за принципом першої важливості.

Параметри, реалізовані на сервері:

- Зберігання, захист і доступ до даних;

- Робота над заявками клієнтів,

Порядок повернення клієнту.

Параметри, які можна змінити на клієнті:

- Інтерфейс, який надає користувачеві графічний досвід;

- Запит на допомогу сервера і подальша доставка запиту;

- Отримання результатів запитів і відправка додаткових команд (запити на додавання, оновлення інформації або видалення групи даних).

Такий тип системи дозволяє брати участь у кількох ідентичних проектах, що в нашому випадку сприяє розширенню системи та дозволить використовувати її в майбутньому в різних компаніях. Крім того, у поєднанні з попередньо визначеною базою даних це дозволяє легко налаштувати різні компоненти системи, не змінюючи код програми, натомість вносячи лише зміни в базу даних.

У результаті, вивчивши всі вищезазначені підходи до розробки програмного забезпечення для нашої системи автоматизації, включаючи швидкість, можливість налаштування та простоту побудови та обслуговування, ми можемо зробити висновок, що найефективнішим підходом буде «архітектура клієнт-сервер».

Оскільки ми обрали клієнт-серверний дизайн програми, міні-комп'ютер буде виконувати роль клієнта, а сервер буде реалізований на Python і функціонуватиме як передача даних між базою даних, нейронною мережею та клієнтом.

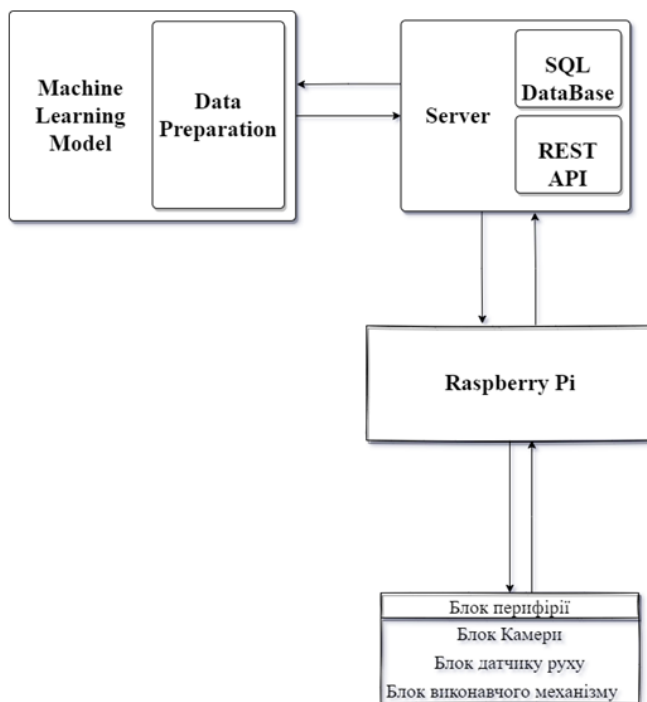


Рис. 4. Блок схема архітектури застосунку

Схема складається з чотирьох основних блоків.

- Raspberry Pi – блок, що відноситься до клієнтського компонента
- Сторона сервера
- Модель машинного навчання (модель ML) – блок, який містить модель для розпізнавання та навчання, а також попередньої обробки даних.
- Периферійний блок - зовнішні компоненти

Компоненти Raspberry Pi та периферійні пристрої — це фізичні компоненти, які розташовані безпосередньо на інсталяції, інші компоненти — це програмні додатки, розташовані на сервері або в «хмарі». Raspberry Pi та його периферійні пристрої взаємодіятимуть один з одним через паралельну шину даних у синхронному режимі. Тобто до отримання сигналу від датчика руху периферійний блок буде залишатися нерухомим.

Завдяки цій взаємодії «Сервер», «Модель машинного навчання» та «Raspberry Pi» будуть виконуватися через Rest API, який є підходом, який використовує HTTP-запити.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В результаті можна зробити висновок, що система контролю та управління доступом не є останньою розробкою і вже досягнута в цьому напрямку, однак остаточного вирішення проблеми захисту швидкості з точки зору контролю доступу досі немає. Оскільки швидкість у напрямку нахилу велика, починають використовуватися картки або мітки, які можна підробити. При збільшенні глибини захисту починають виникати проблеми з налаштуваннями системи і втрата персональних даних. Наразі в РК-телевізорах відсутні опції з функцією розпізнавання обличчя, хоча вони можуть вирішити проблеми швидкості та безпеки.

Література

1. NEC. Facial Recognition [Електронний ресурс]. // Режим доступу: https://u.nec.com/solutions/security/technologies/face_recognition.html (дата обращения: 12.05.2018).

2. Neurotechnology. VeriLook SDK [Электронный ресурс]. // Режим доступа: <http://www.neurotechnology.com/> (дата звернения: 13.11.2024).
3. Techniques and Challenges of Face Recognition: A Critical Review [Электронный ресурс]. // Режим доступа: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (дата звернения: 13.11.2024).
4. TechniquesandChallengesof Face Recognition: A Critical Review [Электронный ресурс]. // Режим доступа: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (дата звернения: 13.11.2024).
5. AndreaF. Abate, Nappi Nappi, Riccio Riccio, Gabriele Sabatino 2D and 3D face recognition: A survey Pattern Recognition Letters, 28 (14) (2007), pp. 1885-1906
6. FaceNet: A Unified Embedding for Face Recognition and Clustering [Электронный ресурс]. // Режим доступа: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf (дата звернения: 13.11.2024).

References

1. NEC. Facial Recognition [Elektronnyi resurs]. // Rezhym dostupu: https://u.nec.com/solutions/security/technologies/face_recognition.html (data obrashcheniya: 12.05.2018).
2. Neurotechnology. VeriLook SDK [Elektronnyi resurs]. // Rezhym dostupu: <http://www.neurotechnology.com/> (data zvernennia: 13.11.2024).
3. Techniques and Challenges of Face Recognition: A Critical Review [Elektronnyi resurs]. // Rezhym dostupu: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (data zvernennia: 13.11.2024).
4. TechniquesandChallengesof Face Recognition: A Critical Review [Elektronnyi resurs]. // Rezhym dostupu: <https://www.sciencedirect.com/science/article/pii/S1877050918321252> (data zvernennia: 13.11.2024).
5. AndreaF. Abate, Nappi Nappi, Riccio Riccio, Gabriele Sabatino 2D and 3D face recognition: A survey Pattern Recognition Letters, 28 (14) (2007), pp. 1885-1906
6. FaceNet: A Unified Embedding for Face Recognition and Clustering [Elektronnyi resurs]. // Rezhym dostupu: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf (data zvernennia: 13.11.2024).

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Антонюк Владислав Русланович

Тема: Метод автоматизованого керування реєстрацією людей у приміщенні

Спеціальність: 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»

Обсяг кваліфікаційної роботи:

Кількість сторінок записки 85

1. Короткий зміст роботи та прийнятих рішень: Метою роботи є розробка системи автоматизованого керування реєстрацією людей у приміщенні
2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню
3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проаналізовані існуючі методи, зроблено висновки щодо актуальності розробки. У другому розділі проведена розробка моделі автоматизації системи контролю та керування доступом. Наведено опис характеристик керування системою розпізнавання обличчя. Виконано обрання платформи для створення локальної системи автоматизації. Зроблено проектування застосунку, а також обрання бази даних. У третьому розділі було розглянуто дослідження існуючих систем розпізнавання осіб, їх плюси і мінуси, дизайн і особливості додатків. Було проведено аналіз цього, щоб знайти найбільш відповідний дизайн для впровадження, що призвело до рішення використовувати FaceNet. У четвертому розділі проілюстровано ефективність будь-якого оптимального алгоритму пошуку на наборі багатовимірних векторів. Запропоновано альтернативний оптимальний метод пошуку на основі векторної класифікації
4. Позитивні сторони роботи: розроблено систему автоматизованого керування реєстрацією людей у приміщенні.

5. Негативні сторони роботи: у роботі недостатньо уваги приділяється аналізу існуючих технічних рішень, наявні стилістичні помилки

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації


7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: відсутні

9. Оцінка дипломної роботи: задовільно (3,50/D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Підченко
Сергій Константинович, завідувач кафедри
ТМІТ, ДТН, професор

“ 20 ” 12 2024 р.

 (підпис)

Завідувачу кафедри АКІТтаР
д-ру техн.наук, проф. Мартинюку В.В.

Антонюк Владислав Русланович

ІІБ здобувача вищої освіти

ФІТ, 2 курс, групи АКІТРМ-23-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений(а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (StrikePlagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

02.12.2024

дата



підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав АНТОНЮК

Співавтор:

Назва: МКР Антонюк

Науковий керівник: Юрій ФОРКУН

Підрозділ: Кафедра автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

Коефіцієнт подібності 1: 0.2%

Коефіцієнт подібності 2: 0.2%

Мікропробіли: 3

Заміна букв: 1

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-20 11:10:27.0

Після аналізу Звіту подібності констатую наступне:

Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.

Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.

Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедур. Таким чином робота не приймається.

Обґрунтування:

2024-12-20

Дата


експерт

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 7.0%

Словники перевірки: en_US, ru_RU, ua_UA. Помилки в документах: 9%

ID: 161824 Назва: МКР Метод автоматизованого керування реєстрацією людей у приміщенні Додано в БД: 2024-12-20 Автора: Владислав АНТОНЮК Керівники: Юрій ФОРКУН Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	92932	843	6789 (7%)	88 (10%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМПІСІЇ
КАФЕДРИ АВТОМАТИЗАЦІЇ, КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ ТА
РОБОТОТЕХНІКИ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод автоматизованого керування реєстрацією людей у приміщенні

Автор: Антонюк Владислав Русланович

Спеціальність: 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка

Освітня програма: Освітньо-професійна програма «Автоматизація та комп'ютерно-інтегровані технології»

Науковий керівник: Форкун Юрій Вікторович, кандидат технічних наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої й електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того, як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) у тексті кваліфікаційної роботи системами перевірки на плагіат виявлено схожість з деякими документами в частині загальноживаних обов'язкових словосполучень у стандартних бланках (титулка, відомість документів), у структурі змісту, назвах розділів/підрозділів тощо, у назвах публікацій у переліку джерел посилання;

2) усі запозичення є фрагментарними або мають належним чином оформленні посилання;

3) виявлені модифікації тексту не впливають на відсоток схожості.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів ідентичності/схожості, складає 0,25% і адресується до 3 джерел, що, з урахуванням наведених обґрунтувань, відповідає характеру теми і свідчить на користь кваліфікаційної роботи.

Завідувач кафедри

Гарант освітньої програми

Керівник кваліфікаційної роботи

Валерій МАРТИНЮК

Валерій МАРТИНЮК

Юрій ФОРКУН