НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
„КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО”

ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ
КАФЕДРА ЕЛЕКТРОННИХ ПРИСТРОЇВ ТА СИСТЕМ

До захисту допущено
Завідувачка кафедри

_____ __Юлія ЯМНЕНКО___
(підпис) (ім‘я ПРІЗВИЩЕ)

"_____" _____ 2021 р.

Дипломний проєкт

на здобуття першого (бакалаврського) рівня вищої освіти

Спеціальність ___171 Електроніка_____
(код та назва спеціальності)
Спеціалізація Електронні прилади та пристрої

на тему: Автономна система контролю доступу в приміщення_

Виконав (-ла): студент (-ка) ____IV_____ курсу, групи ДЕ-71
_____Ольга ЄВСЕВ’ЄВА_____ _____
(ім‘я ПРІЗВИЩЕ) (підпис)

Керівник _старший викладач, Ганна САРИБОГА_ _____
(посада, науковий ступень, вчене звання, ім‘я ПРІЗВИЩЕ) (підпис)

Консультант _____ _____
(назва розділу) (посада, науковий ступень, вчене звання, ім‘я ПРІЗВИЩЕ) (підпис)

Рецензент _доцент, кт.н., доц. Павло ПОПОВИЧ_____ _____
(посада, науковий ступень, вчене звання, ім‘я ПРІЗВИЩЕ) (підпис)

Консультант
з нормоконтролю доцент, к.т.н., доц. Павло САФРОНОВ____ _____
(посада, науковий ступень, вчене звання, ім‘я ПРІЗВИЩЕ) (підпис)

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань
Студент _____
(підпис)

Київ – 2021 року

№ з/п	Формат	Позначення	Найменування	Кількість аркушів	Примітка
1			Завдання на дипломний проєкт	2	
2	А4	ДП.ДЕ-71.003 ПЗ	Пояснювальна записка	53	
3	А1	ДП.ДЕ-71.003 Е1	Схема електрична структурна	1	
4	А1	ДП.ДЕ-71.003 СА	Схема алгоритму	1	
5	А1	ДП.ДЕ-71.003 СА	Схема алгоритму	1	

Зм.	Арк	П.І.Б.	Підп.	Дата	ДП. ДЕ-71. 007.ВП			
Розроб.		Ольга ЄВСЕВ'ЄВА			Автономна система контролю доступу в приміщення *Відомість дипломного проєкту*	Літ.	Арк.	Аркушів
Перевірив		Ганна САРИБОГА					1	1
						КПІ ім. Ігоря Сікорського, ФЕЛ, ЕПС, гр. ДЕ-71		
Н.контр.		Павло САФРОНОВ						
Затверд.		Ганна САРИБОГА						

Національний технічний університет України
“Київський політехнічний інститут
імені Ігоря Сікорського”

Факультет електроніки
(повна назва)

Кафедра електронних пристроїв та систем
(повна назва)

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 171 Електроніка
(шифр і назва)

Спеціалізація Електронні прилади та пристрої

ЗАТВЕРДЖУЮ

В.о. завідувачка кафедри

_____ Юлія ЯМНЕНКО
(підпис) (ім‘я ПРІЗВИЩЕ)

"_____" _____ 2020 р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ СТУДЕНТУ

Ользі ЄВСЕВ'ЄВІЙ
(ім‘я ПРІЗВИЩЕ)

1. Тема проєкту автономна система контролю доступу в приміщення

Керівник проєкту старший викладач Ганна САРИБОГА,
(посада, науковий ступень, вчене звання, ім‘я ПРІЗВИЩЕ)

затверджені наказом по університету від «24» травня 2021 року № 1316-с
2. Термін подання студентом проєкту 15.06.2021
3. Вихідні дані до проєкту Raspberry Pi4, web-камера, Logitech, Python, Open CV

4. Зміст пояснювальної записки (перелік завдань, які потрібно розробити)
1. Провести аналітичне дослідження систем контролю доступу і на його основі здійснити побудову моделі предметної області;
2. Запропонувати рішення щодо реалізації програмно-апаратної платформи , яка забезпечує виконання пред’явлених вимог до систем персонального доступу;
3.Розробити структурну, функціональну схему системи з підбором та обґрунтуванням комплектуючих ;

4. Розробити програмне забезпечення системи технічного зору
5. Отримати експериментальні дані ефективності запропонованого рішення

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) _схема електрична структурна, схема алгоритму_____

6. Консультанти розділів проєкту

Розділ	Ім'я ПРІЗВИЩЕ, посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Технічний			

7. Дата видачі завдання 20 травня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломного проєкту	Строки виконання етапів проєкту	Примітка
1	Огляд існуючих систем	06.01.2021	виконано
2	Дослідження існуючих прототипів	14.03.2021	виконано
3	Розробка семи системи	16.04.2021	виконано
4	Розробка програмного забезпечення	02.05.2021	виконано
5	Обробка результатів дослідження	10.06.2021	виконано
6	Оформлення дипломного проекту	15.06.2021	виконано

Студент _____ Ольга Євсев'єва
(підпис) (ім'я ПРІЗВИЩЕ)

Керівник проєкту _____ Ганна САРИБОГА
(підпис) (ім'я ПРІЗВИЩЕ)

А Н О Т А Ц І Я

В дипломному проєкті представлено інформацію отриману в результаті дослідження про системи безпеки, системи контролю доступом зокрема.

Показано використання системи контролю доступу як автономного складника системи обмеження доступу з використанням пристрою Raspberry Pi,(+овпенсCIBI + алгоритм) а не як частини системи безпеки загалом.

Мета роботи – розробити ефективну систему контролю та управління доступом на базі системи технічного зору з використанням алгоритмів розпізнавання обличчя. Метод дослідження – експериментальний.

Для досягнення мети було розроблено програмно-апаратний комплекс, який в автоматичному режимі фіксує інформацію про зареєстрованих осіб та записує історію їхніх проходжень через пункт пропуску.

Також створено мобільний додаток для користувачів, які мають особливий доступ, де інтерфейс дозволяє переглядати список зареєстрованих користувачів і повну історію їх фіксувань камерою.

A N N O T A T I O N

The diploma project presents information obtained as a result of research on security systems, access control systems in particular.

The use of the access control system as an autonomous component of the access restriction system using the Raspberry Pi device is shown, and not as part of the security system as a whole.

The purpose of the work is to develop an effective system of access control and management based on a system of technical vision using facial recognition algorithms. The research method is experimental.

To achieve this goal, a software and hardware complex was developed that automatically records information about registered persons and records the history of their passage through the checkpoint.

There is also a mobile application for users with special access, where the interface allows you to view the list of registered users and the full history of their recordings by the camera.

Keywords: access control system, Raspberry Pi, face recognition.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ — Програмне забезпечення

СКД — Система контролю доступу

АСКД — Автоматизована система контролю доступу

ВСТУП

Поява систем контролю доступу в приміщення тісно пов’язана з прагненням забезпечити високий рівень безпеки та надійності охорони важливих об’єктів інфраструктури, формування безпечного середовища для кожного відвідувача приміщення та зниження ризиків несанкціонованого проникнення небажаних елементів у приміщення під охороною.

Автономізація систем контролю покликана зменшити людський фактор у забезпеченні вільного доступу зареєстрованих користувачів з правом доступу до приміщень та інших об’єктів інфраструктури.

Саме завдяки зручності та керованості системи контролю й управління доступом нині є невід’ємною частиною систем забезпечення безпеки осіб, які перебувають у приміщенні. Вони дають змогу обмежити, впорядкувати контроль доступу у різні приміщення, при цьому фіксуючи інформацію про пересування людей, для подальшого використання цієї інформації для моніторингу дій користувачів систем, протидії незаконним діям та захисту конфіденційної інформації

Сучасні СКУД – це не лише апаратне та програмне забезпечення, а повністю продумані системи, що здатні ідентифікувати осіб, керувати доступом, зберігати та аналізувати отримані дані.

Контроль доступу – це вибіркове обмеження доступу до певного місця, кімнати, ресурсу або установи. Для отримання доступу до обмеженого місця розташування, фізична особа, зазвичай, має пройти авторизацію або отримати дозвіл на вхід.

Вадами наявних на ринку СКУД є висока вартість експлуатації та необхідність постійно взаємодіяти з постачальником рішення, також наявні СКУД здебільшого не є універсальними, тобто потребують адаптації під кожне завдання та тип приміщення, а також не є ергономічними для користувачів. Оскільки наявні СКУД не гарантують 100% безпеки та мають вищевказані вади, постала проблема розробки системи, яка б комплексно вирішувала

завдання швидкого встановлення та розгортання, зі зрозумілим для пересічного користувача та з індивідуальними налаштуваннями для підвищення рівня безпеки. Додатковими можливостями цієї системи буде надання можливості користувачу інтерфейсу для перегляду результату роботи.

Перелік основних завдань, що мають бути реалізовані у цій системі:

- візуальна ідентифікація;
- формування індивідуальних і групових повноважень доступу;
- керування доступом через інтерфейс;
- облік часу.

У цій роботі метою є створення автономної системи контролю доступу в приміщення, у якій реалізовано вищевказані завдання. Також ця система не потребує додаткового інструментарію для взаємодії з користувачем.

1. ПОСТАНОВКА ЗАДАЧІ ДО СИСТЕМИ ДОСТУПУ

Перед початком розробки власного СКУД необхідно проаналізувати наявні рішення, що вже довели власну ефективність у процесі роботи.

За рівнем ідентифікації доступу розрізняють однорівневі та багаторівневі СКУД. У однорівневі СКУД ідентифікація користувача здійснюється за 1 ознакою, а у багаторівневих використовується декілька ознак, серед яких, зокрема аналізуються біометричні дані та код картки) [1].

Залежно від специфіки об’єкта, фінансових можливостей власників об’єкта приміщення може бути оснащено різними СКУД, які мають унікальний фактор аутентифікації, до яких включають паролі, пристрої аутентифікації та біометричні дані [2]

Розроблена система призначена для ідентифікації особи за допомогою пристрою Raspberry Pi, до складу якої входить звичайна веб-камера. Адміністратор має доступ до пристрою, а саме, знаючи пароль і знаходячись в одній локальній мережі, може напряму підключатися до операційної системи через WiFi. Це надає можливість реєструвати для розпізнавання обличчя нову особу, ім’я та набір фото якої зберігатимуться на Raspberry Pi.

Особливістю цієї системи є мобільний додаток, який допоможе адміністратору та користувачам з особливим доступом запрошувати дані у центрального сервера, такі як:

— повну історію фіксувань камерою зареєстрованих осіб;

— список зареєстрованих осіб;

— історію фіксувань камерою окремо для кожної людини в списку.

Окремо можна виділити людей, фото яких внесено для розпізнавання. Їм не надається ніяка можливість контактувати з програмним забезпеченням та системою.

В результаті проектування програмна частина системи складається з:

1) центрального сервера, через який проходять всі запити та відбувається зв'язок з базою даних;

2) компонента, який відповідає за розпізнавання людей;

3) мобільного пристрою, який виступає в ролі інтерфейсу для спілкування з центральним сервером;

4) бази даних, розміщеної на Raspberry Pi, в якій зберігатимуться дані про зареєстрованих користувачів, а саме імена та історія фіксувань камерою.

Зв'язок мобільного додатку з центральним сервером відбуватиметься у випадку підключення до однієї локальної мережі. В такому разі виключно окрема кількість осіб з особливим доступом, в яких встановлено описаний мобільний додаток та є доступ до мережі, зможуть отримувати інформацію з бази даних.

Мобільний додаток було вирішено розробляти з використанням мови програмування Dart та фреймворку Flutter. Компонент розпізнавання – за допомогою мови Python та набору бібліотек, однією з яких є OpenCV. Центральний сервер – з використанням веб фреймворку Flask та мови Python.

— Провести аналітичне дослідження систем контролю доступу і на його основі

— здійснити побудову моделі предметної області;

— Запропонувати рішення щодо реалізації програмно-апаратної платформи , яка забезпечує виконання пред'явлених вимог до систем персонального доступу;

— Розробити структурну, функціональну схему системи з підбором та обґрунтуванням комплектуючих ;

— Розробити програмне забезпечення системи технічного зору

— Отримати експериментальні дані ефективності запропонованого рішення аналітично розрахувати надійність роботи системи.

2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ТА ЇХ АНАЛІЗ

2.1 Специфікація охоронних систем

Загальне визначення системи безпеки об'єкта може бути сформовано виходячи з функціонального призначення.

В поняття «система безпеки» покладено розуміння сукупності засобів та методів підтримання безпечного стану об'єкта, попередження, виявлення та ліквідація загрози життю, інформації та іншим важливих аспектам.

При цьому необхідність забезпечення безпечного стану об'єкта, попередження, виявлення та ліквідація загрози визначаються основними функціями систем безпеки. Ліквідація цих загроз досягається застосуванням спеціальних методів та засобів.

Ускладнення у реальних умовах, що вимагає підвищення рівня безпеки, передбачає розвиток технічних складових систем безпеки.

У більшості випадків розділене застосування спеціальних систем або підсистем не забезпечує достатній рівень безпеки. Тому організація ефективного захисту можливо на основі інтеграції всіх засобів забезпечення безпеки в об'єднаній системі, включаючи в себе наступні елементи:

— Організаційні. Це сукупність організаційно-технічних (забезпечення комп'ютерними приміщеннями, налаштування кабельної системи та ін.) та організаційно-правових (законодавча база, статут конкретної організації) коштів.

— Програмні. Ті програми, які допомагають контролювати, зберігати і захищати інформацію та доступ до неї.

— Технічні (апаратні). Це технічні види пристроїв, які захищають інформацію від проникнення і витоку.

— Змішані апаратно-програмні. Виконують функції як апаратних, так і програмних засобів. [3]

Охоронна система — це набір програмних та апаратних компонентів, основною задачею яких є досягнення безпеки на деякій території, будь то будівля, кімната чи навіть транспортний засіб. Передбачається що система повинна запобігати можливій загрозі здоров'ю або майну людей що знаходяться на захищеній території**.** Поставлені вимоги можуть виконуватися за допомогою сповіщень або спроб запобігти конкретній небезпечній ситуації в автономному чи ручному режимі. [4]

Варто зазначити, що розділення охоронних систем є доволі умовним, оскільки, на практиці кращі результати показують комплексні системи.

2.2 Огляд автоматизованих систем контролю доступу

Система контролю доступу є одним з підтипів охоронних систем та виконує функції пропуску особи до деякої території за наявності досягненого сигналу підтвердження що людина підходить по заданим програмним та апаратним комплексом вимогам. Під автоматизованою системою розуміємо реалізацію контролю доступу таким чином, щоб була відсутня потреба постійного нагляду за ходом роботи технічних засобів, тобто комплекс коректно функціонував без втручання оператора. [5]

Основною з задач які ставляться перед системою контролю доступу є правильне проведення авторизації та автентифікації користувачів. Це може досягатися шляхом перевірки різного набору даних, одними з яких є:

— інформаційні магнітні картки, NFC або RFID мітки;

— біометричні дані, такі як лице особи або відбитки пальців;

— пароль;

Можна виділити цілий спектр випадків в яких можна використати систему контролю доступу, наприклад, для:

— надання права фізичного доступу до обмеженої території для працівників або зареєстрованих осіб;

— побудови багатошарової системи доступу з різними рівнями доступу до об’єктів;

— збору інформації про час фіксування осіб, що пройшли або намагалися пройти пункт контролю доступу;

— для побудови звітів про відвідування обмеженої території різними особами.

СКД можна поділити на основні підтипи:

1) автономні — система функціонує самостійно, а тому немає потреби постійного втручання в роботу програмної чи апаратної частини системи оператора або адміністратора;

2) мережеві — система потребує постійного нагляду оператором, інформація про роботу постійно передається в центральний модуль збору даних для контролю доступу;

3) універсальні — полягає в поєднанні як автономного так і мережевого підходу.

Задачею оператора або адміністратора можуть бути облік та обробка зібраної системою контролю доступу інформації, такої як особисті дані користувачів, фото, часу фіксувань осіб чи транспорту на пункті пропуску. Також до повноважень можна віднести реєстрацію та надання рівню доступу, видачу нових перепусток, контролю стану роботи різних пристроїв системи. У випадку великої кількості виконуваних функцій часто наймаються кілька працівників, які розподілено між собою виконують описані задачі.

2.2.1 Термінал контролю доступу SpeedFace V5

Термінал контролю доступу по геометрії обличчя є самодостатнім готовим пристроєм для створення автоматизованого доступу на деяку територію приміщення, офісу, або навіть цілого підприємства. Таку систему можна використовувати для обмеження доступу сторонніх осіб. До того ж однією з особливостей є можливість зібрати інформацію про зареєстрованих

осіб та вивести у вигляді звітів. Пристрій SpeedFace V5 може виконувати пропуск в автоматичному режимі, вручну, а також існує варіант роботи в складі СКД BioTime 8.0. Програмне забезпечення при покупці включається в комплект з пристроєм. Пристрій представляє невеликий термінал з сенсорним дисплеєм.

Рис. 2.1. Вигляд пристрою SpeedFace V5

Основні особливості пристрою:

— кілька видів ідентифікації осіб: за RFID картками, по геометрії обличчя та за відбитками пальців;

— є можливість підключення через кабель Ethernet і в результаті управляти терміналом на великих відстанях;

— неможливо пройти через термінал ще раз одній і тій же особі поки вона не вийде з обмеженої території;

— максимально можлива дистанція, на якій система розпізнає лице особи, складає приблизно три метри;

— значна кількість даних, які можуть зберігатися та використовуватися як база для зареєстрованих користувачів, а саме: 6000 знімків обличчя осіб, 10000 відбитків пальців;

— надання безкоштовних інструментів розробника – для можливості об’єднання з сторонніми системи.

Ідентифікація осіб пристроєм SpeedFace V5 працює за простим набором принципів: в базу даних вносяться знімки осіб співробітників, які прив'язуються в базі до їх облікових записів. Зразу після цього співробітник має змогу проходити через контрольні точки, згідно з правами доступу, що було надано при реєстрації — кожного разу при входженні відбувається ідентифікація власника пропуску. В результаті системою створюються так звані тимчасові розклади можливості проходу. Ці створені розклади присвоюються до відповідних груп зареєстрованих працівників. Кожен раз, коли особа перетинає один із контрольних пунктів, то система аналізує надані цьому співробітнику права доступу та приймає рішення по пропуску людини, а в цей момент базі даних фіксується час та напрямок проходу та зона, в яку людина потрапила. Ось чому СКД завжди знає де знаходиться конкретний співробітник в даний момент часу, коли він потрапив до якої зони та коли з неї вийшов.

Як уже згадувалося вище, система контролю доступу SpeedFace V5 має змогу працювати з трьома різними типами ідентифікаторів, а саме: геометрія обличчя особи, відбитки пальців, безконтактні картки. Основною особливістю є можливість побудова варіацій двох і трьох-рівневої верифікації співробітників заради кращої безпеки обмеженої території.

Далі наведено основні такі можливі підходи:

— геометрія обличчя особи та відбиток пальця;

— геометрія обличчя особи та безконтактна картка;

— геометрія обличчя особи та безконтактна картка та відбиток пальця.

Тобто якщо, наприклад, обрана багаторівнева верифікація за допомогою геометрії обличчя особи та відбитку пальця, то співробітник повинен спочатку пройти ідентифікацію по геометрії обличчя особи, а після цього, після успішної ідентифікації, піднести свій палець до сканера відбитків. Якщо в результаті перевірки наданих даних та прав доступу цього користувача системою буде видано сигнал про успішне проходження даних кроків, то особа буде пропущена далі.

Для пропуску особи можуть використовуватися будь-які види електрозамків, шлагбауми, турнікети. Періодичність повторних зчитувань обличчя системою, як і деякі інші параметри, можуть регулюватися в налаштуваннях апаратної частини пристрою.

2.2.2 Термінал контролю доступу SFace900

Мульти біометричний термінал контролю доступу до біометричних даних особи, відбитків пальців та безконтактної картки SFace900 (рис 2.2) є системою обмеженого доступу, що містить автономну пам'ять для збереження 3000 шаблонів осіб, 3000 відбитків пальців і 10000 безконтактних карт.

Рис. 2.2. Вигляд пристрою SFace900

Це один із перших терміналів, що оснащений високопродуктивною камерою, яка розрахована для роботи системи на вулиці. Одним із особливостей пристрою є оснащення останньою платформою та алгоритмом ZKTeco, які надають клієнтам зручний простий користувацький інтерфейс. А також завдяки покращеному алгоритму обробки обличчя осіб і технології мульти біометричної перевірки рівень точної ідентифікації особи забезпечує дуже високі показники.

Особливості терміналу контролю обмеженого доступу SFace900 та користувацького інтерфейсу:

— встановлення системи на вулиці (за умови світлового потоку до 12,000 люкс);

— виявлення та відкидання фальшивих облич осіб, що значно підвищує рівень безпеки при перевірці;

— висока швидкість перевірки особи;

— додаткова резервна батарея, що вбудована в пристрій та забезпечує роботу у випадку відключення електроенергії протягом близько 4 годин, для роботи в критичних ситуаціях;

— багатомовний інтерфейс.

2.2.3 Термінал контролю доступу Multibio700

Мульти біометричний термінал Multibio700 (рис. 2.3) використовується в системах контролю обліку робочого часу працівників для доступу в приміщення з обмеженим доступом по таких ідентифікаторах як: геометрія обличчя, відбиток пальця, безконтактна картка та код.

Рис. 2.3. Вигляд пристрою Multibio700

Пристрій фіксує відносну позицію, розмір і форму очей особи, носа, та деяких інших точок обличчя та формує з цих даних біометричний шаблон для подальшого розпізнавання, а точніше порівняння із базою даних. Ідентифікація користувача проходить швидко та точно в межах однієї секунди. Особливістю пристрою є інфрачервоне підсвічування, що дозволяє проводити ідентифікацію в умовах низького рівня освітленості.

Термінал по геометрії обличчя використовується для прямого управління електронним замком. В даному випадку Multibio700 є контролером і зчитувачем в одному корпусі. Така будова забезпечує зручний і простий монтаж біометричної системи.

Також можлива інтеграція пристрою в інші системи контролю доступу з використанням інтерфейсу Wiegand. Пристрій Multibio700 є зчитувачем і передає код ідентифікації користувача через інтерфейс на контролер. Така побудова забезпечує високий рівень безпеки точки контролю проходу.

Крім функцій обмеженого доступу до приміщення термінал виконує також функцію обліку робочого часу для кожного працівника. Автономна пам'ять системи розрахована на приблизно 100000 подій, а безкоштовне програмне забезпечення, що поставляється в комплекті, дозволяє формувати звіти по робочому часу.

2.3 Аналіз методів розпізнавання облич

2.3.1 Розпізнавання осіб на основі OpenCV.

Робота базового процесу розпізнавання осіб:

1. Виявлення особи на зображенні.
2. Виділення особливостей на обличчі.
3. Перетворення для порівняння з особами в базі даних.
4. Висновок (визначення відповідності між особами).

Для виявлення осіб, використано метод Віоли-Джонса .

Для ідентифікації осіб можна використано модель ASM (Active Shape Models) . Основна ідея полягає в обліку статистичних зв'язків між розташуванням антропометричних точок обличчя . На кожному зображенні особи точки пронумеровані в однаковому порядку. За їх взаємного розташування здійснюється порівняння осіб.

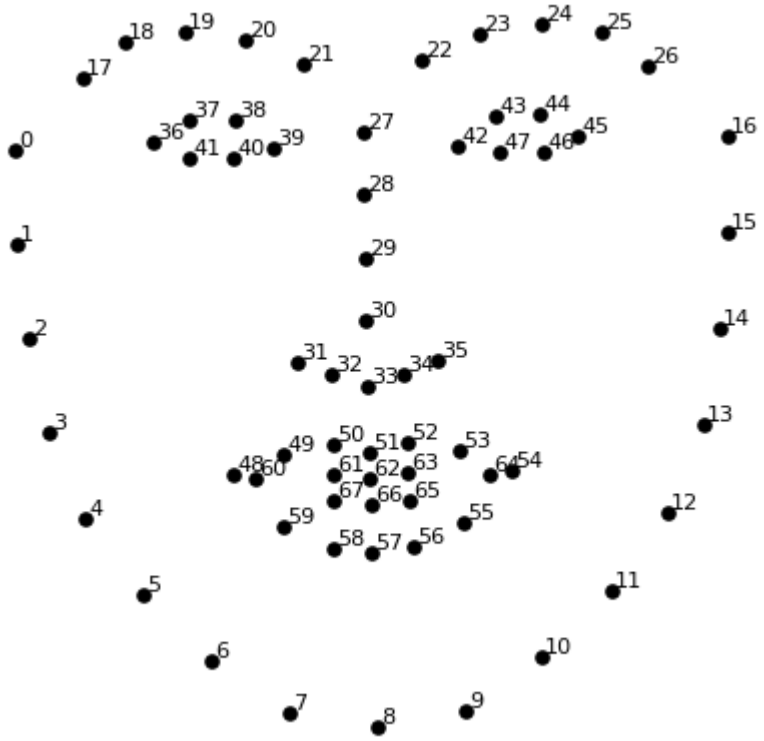

Рис. 2.4 Зображення точок обличчя

Для порівняння осіб можна використовувати точковий 2D-каркас одного і того ж положення особи відносно камери. Але більш кращий у використанні для цього буде точковий 3D-каркас .

2.3.2 Захоплення відеопотоку з камери і виділення обличчя

На основі фрагментів програм отримано додаток, який забезпечує захоплення відеопотоку з камери і виділяє обличчя (використовуючи Haar-Cascade класифікатор).

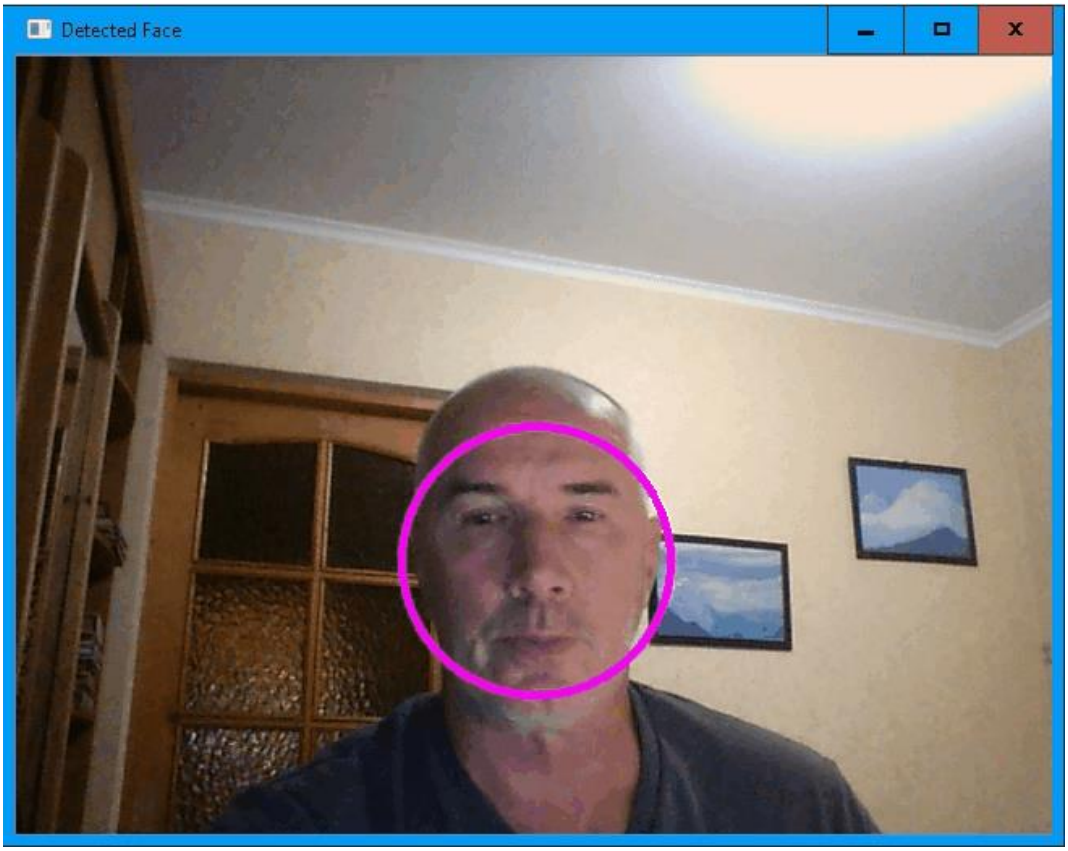

Рис. 2.5 Зображення виділення обличчя з відеопотоку

2.3.3 Виділення особливих точок особи

Додаток створено на основі C ++ code для OpenCV Facemark

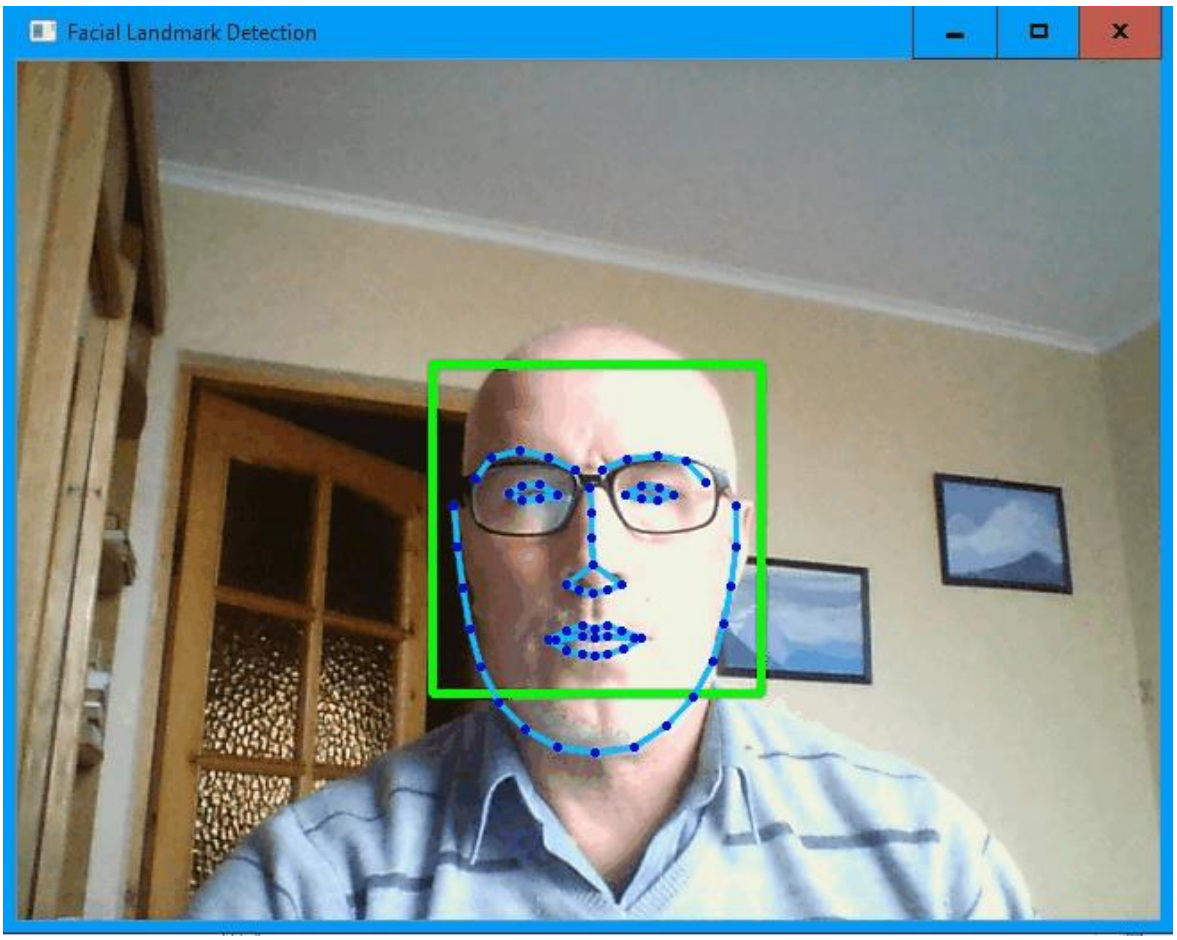

Рис. 2.6 Зображення виділення особливих точок особи

2.3.4 Вибір ознак для фільтрації зображень і розпізнавання осіб

Точковий каркас обличчя особи відображається по різному в залежності від об'єктивних і суб’єктивних факторів.

Об'єктивні чинники - стан особи відносно камери.

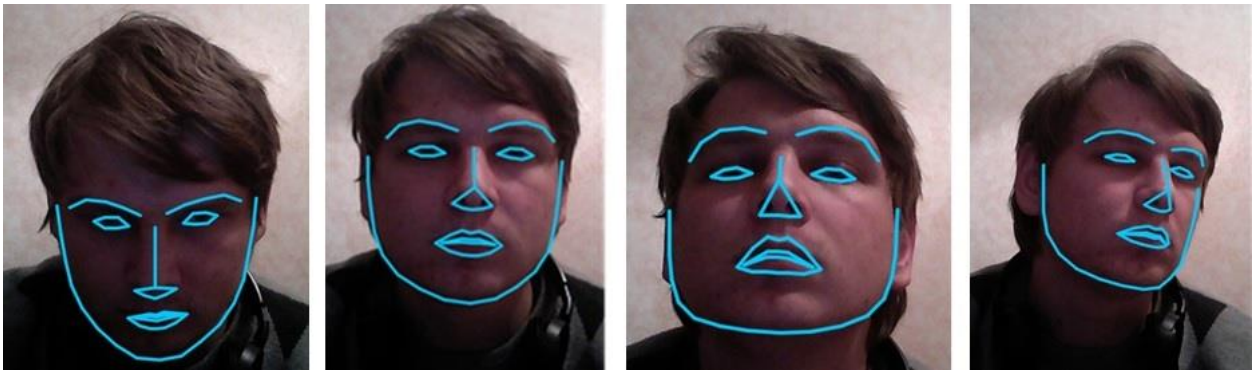

Рис. 2.7 Зображення вибору ознак для фільтрації і розпізнавання осіб

Суб'єктивні чинники - нерівномірне або слабке освітлення, спотворення обличчя внаслідок емоцій, прищурення ока і т.п. У цих випадках точковий каркас може бути некоректним, точки можуть навіть бути відірвані від імені:

Рис. 2.8 Зображення некоректного відображення каркасу

При відеозахопленні іноді проскакують і такі зображення. Їх потрібно фільтрувати - як при навчанні так і при розпізнаванні.

Деякі з точок є найбільш стабільними і інформативними. Вони жорстко прив'язані до обличчя, незалежно від його положення щодо камери. Крім того, вони добре характеризують специфіку особи. Ці точки можуть бути використані як основа для моделювання системи ознак.

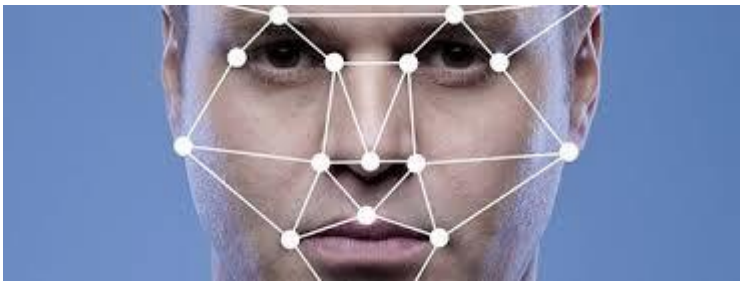

Рис. 2.9 Зображення некоректного відображення каркасу

Для порівняння осіб можна використовувати точковий 2D каркас одного і того ж положення обличчя особи. Фронтальне становище особи щодо камери є найбільш інформативним.

Всі ознаки (відстані) повинні бути безрозмірні (нормалізованності), тобто, співвіднесені до якогось розміру (відстані). Допускаємо, що найбільш підходить для цього розмір - відстань між центрами кутових точок очей.

Для порівняння візьмемо ознаку у першому наближенні

Припускаючи, що відстань від верхньої точки перенісся до нижньої точки підборіддя. Судячи з фото ця ознака може істотно відрізнятися для різних осіб.

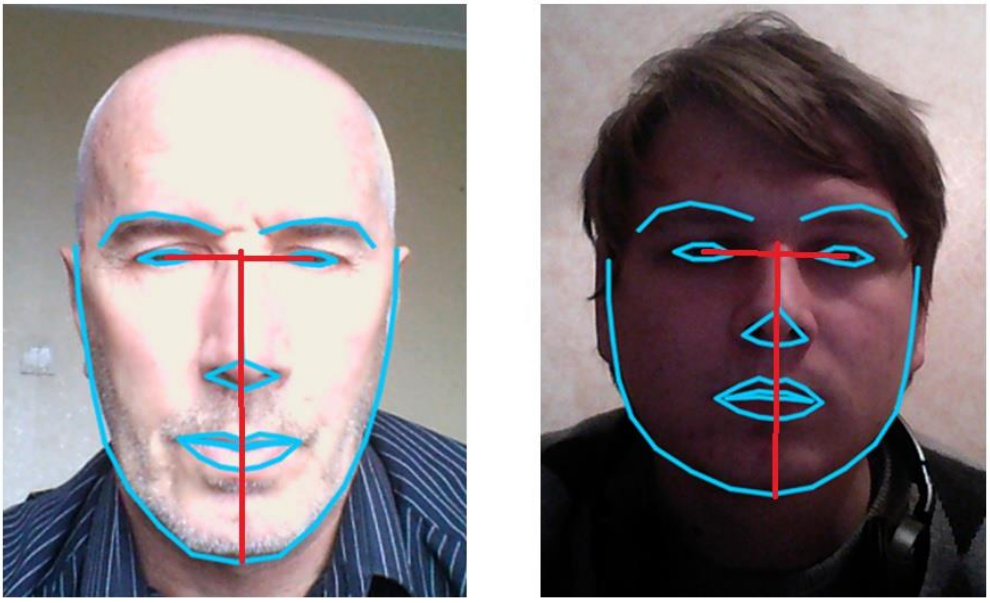

Рис. 2.10 Зображення відмінності виявлення осіб

Отже, перш ніж формувати ознаки для навчання і порівняння, необхідно відфільтрувати отримані відеозахопленні точкові каркаси осіб, які з суб'єктивних чи об'єктивних причин не мають правильне фронтальне зображення обличчя.

Ми залишаємо тільки ті точкові каркаси, які проходять за такими ознаками:

- Пряма, яка проходить через крайні точки очей (лінія очей), перпендикулярна прямий, яка проходить через крайні точки носа (лінія носа).

- Лінія очей паралельна прямій, яка проходить через точки куточків рота (лінія рота).
- Дотримується симетрія зазначених вище точок щодо лінії носа.
- Кутові точки очей (зовнішні і внутрішні) знаходяться на одній прямій.

Приклад фронтальних зображень, які проходять за всіма ознаками:

Рис. 2.11 Зображення фронтальні, які задовольняють систему

Приклад зображень, які фільтруються:

Рис. 2.12 Зображення які не фільтруються

2.3.5 Алгоритм розпізнавання осіб по 2D-каркасу точок

Координати точок каркаса особи спочатку задаються в системі координат, яка прив'язана до верхньої лівої точці вікна. При цьому вісь Y направлена вниз.

Для зручності визначення ознак використовуємо для користувача систему координат, вісь X якої проходить через відрізок між центрами очей, а вісь Y - перпендикулярно цьому відрізку через його середину в напрямку вгору. Координати (від -1 до +1) нормальні – співвіднесені з відстанню між середніми точками очей.

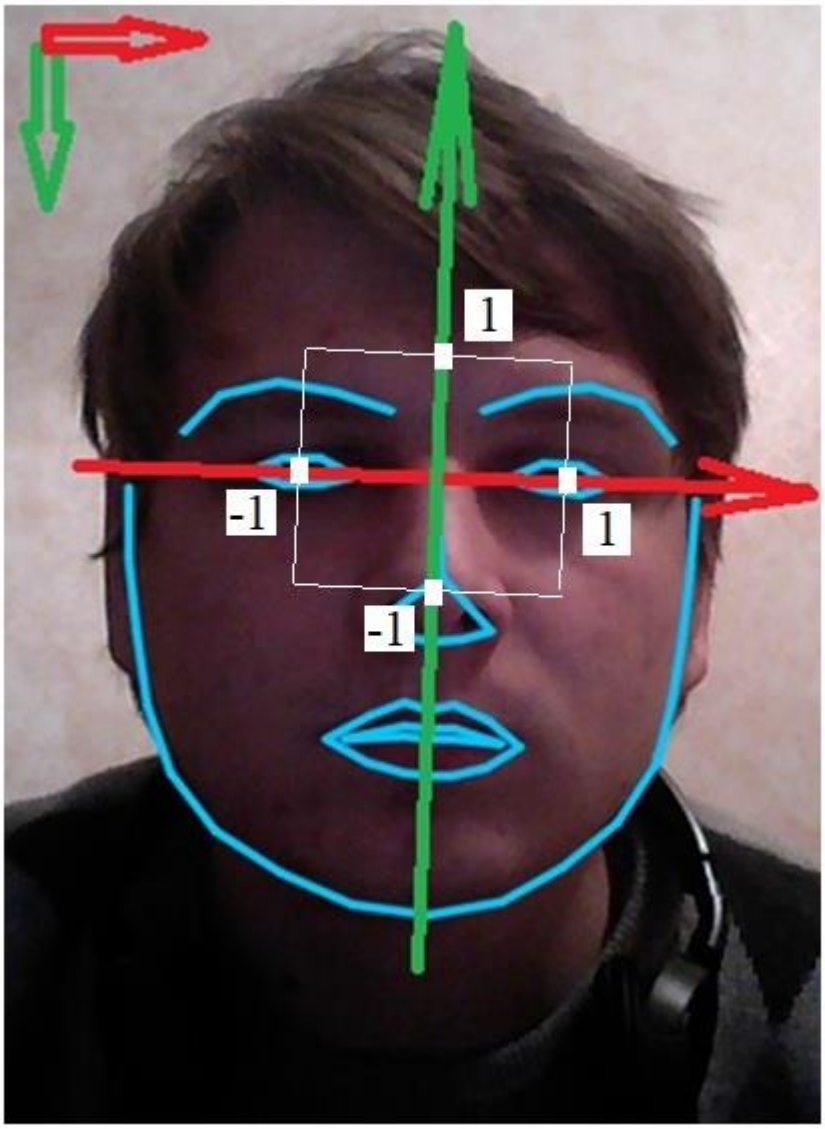

Рис. 2.13 Зображення розпізнавання по 2D каркасу

2.3.6 Програма порівняння осіб за однією ознакою

В якості ознаки береться відстань між точками перенісся і підборіддя. Ознака, нормалізований, визначається в системі координат ставленням: . При навчанні програми ознака для конкретної особи визначається

числом, яке висвічується поряд з відслідковується особою (ця частина коду в програмі закоментований). При розпізнаванні значення ознаки порівнюється з введенням в програму конкретним ознакою для кожної особи. При позитивному результаті порівняння поруч з особою з'являється його ідентифікатор.

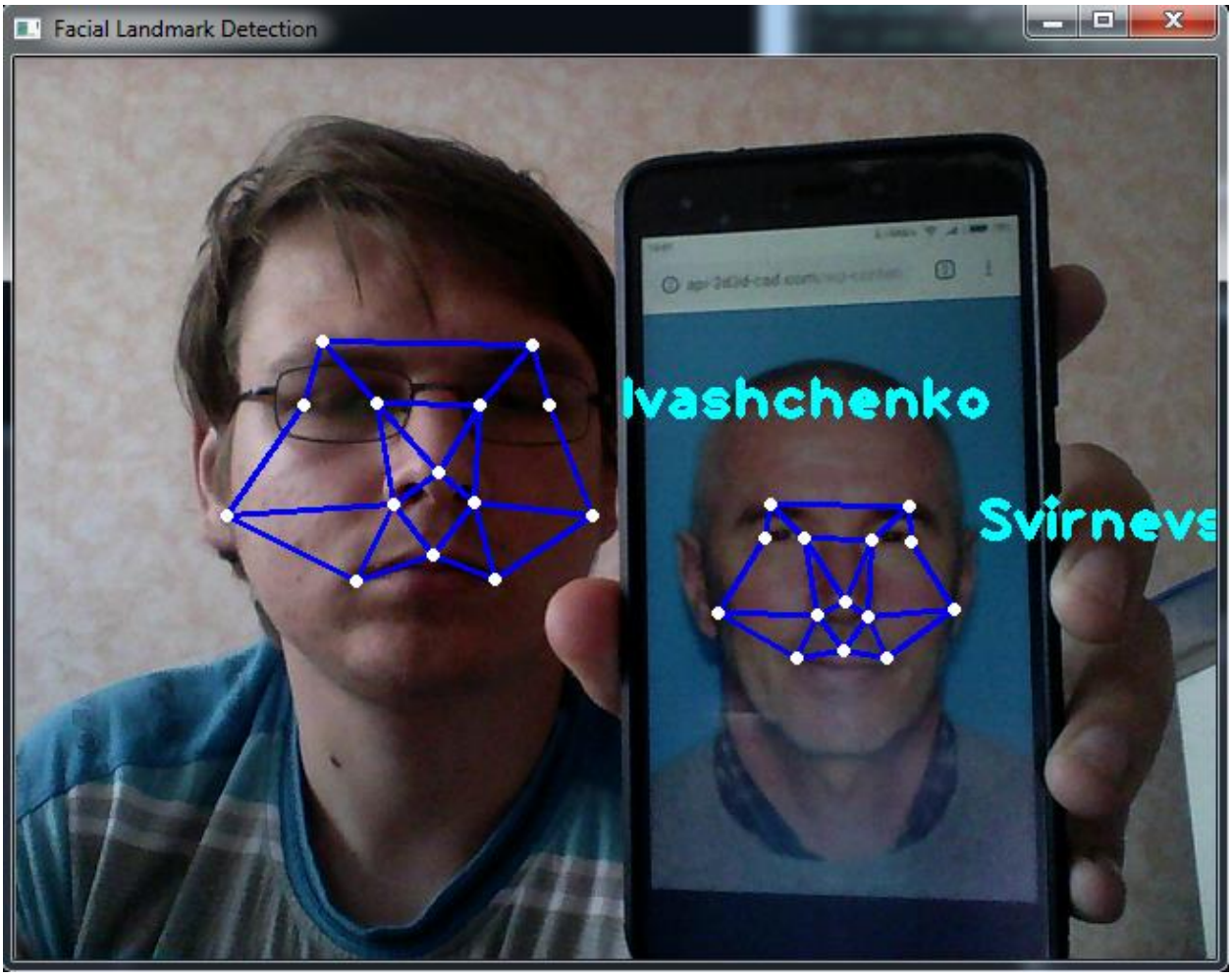

Рис. 2.14 Зображення порівняння осіб за однією ознакою

Програма розпізнає і по фото, на якому особа на 15 років молодше, та й при тому, ще з вусами. Різниця на фото істотне, не кожна людина зможе помітити. Але комп'ютерна програма це вловлює. [8]

Рис. 2.15 Виявлення обличчя з бази з віковими змінами

2.4 Опис розширеного алгоритму розпізнавання Віоли-Джонса

Початковий алгоритм методу розпізнавання Віоли-Джонса було сформульовано ще у 2001 році, але його популярність прослідковується і в сучасному світі, особливо якщо говорити про високу швидкість розпізнавання в реальному часі та про застосування на пристроях з обмеженими обчислюваними можливостями. [6]

Цікавою особливістю алгоритму є те, що в результаті існує можливість розпізнавання облич під невеликим кутом (до 30 градусів).

Якщо говорити про основні принципи, на яких побудовано метод розпізнавання, то можна сформулювати наступні:

— використання зображень в інтегральному представленні, що позитивно впливає на швидкість роботи;

— застосування бустінгу для покращення процесу розпізнавання;

— використання ознак Хаара, за допомогою яких відбувається пошук особливих ознак обличчя;

— використання спеціальних ознак для відкидання областей зображення де немає обличчя;

І хоча навчання класифікатора займає значний час, але основною ключовою особливістю є саме швидкість розпізнавання при достатньо малих похибках, що робить цей алгоритм одним із самих ефективних і малозатратних. [7]

Однією із ідей алгоритму є використання інтегрального представлення, яке дозволяє швидко розраховувати суму яскравостей довільного прямокутника на даному зображенні, при цьому важливо, що час розрахунку не залежить від площі прямокутника.

Інтегральне представлення зображення є матрицею, що збігається за розмірами з вихідним зображенням, тобто кожен піксель дорівнює одному елементу матриці. У кожному її елементі зберігається сума інтенсивностей всіх пікселів, що знаходяться лівіше і вище даного елемента. Елементи матриці розраховуються за такою формулою:

$$I(x,y) = \sum_{x' \le x, y \le y} i(x',y'), \qquad (2.1)$$

де *I(x,y)* — це значення точки *(x,y)* даного інтегрального зображення, а *i(x,y)* — це значення інтенсивності вихідного зображення. Використовуючи інтегральне представлення зображення, обчислення ознак такого ж виду але з різними геометричними параметрами відбувається за ідентичний час. Кожен же елемент матриці *I(x,y)* представляє суму пікселів в прямокутнику від значення *i(0,0)* до *i(x,y)*, а звідси значення кожного елемента *I(x,y)* дорівнює сумі значень усіх пікселів лівіше і вище даного пікселя *i(x,y)*. Важливою особливістю є те, що розрахунок матриці займає лінійний час і є пропорційним числу пікселів на зображенні та обчислюється за наступною формулою:

$$I(x,y) = i(x,y) - I(x-1,y-1) + I(x,y-1) + I(x-1,y). \qquad (2.2)$$

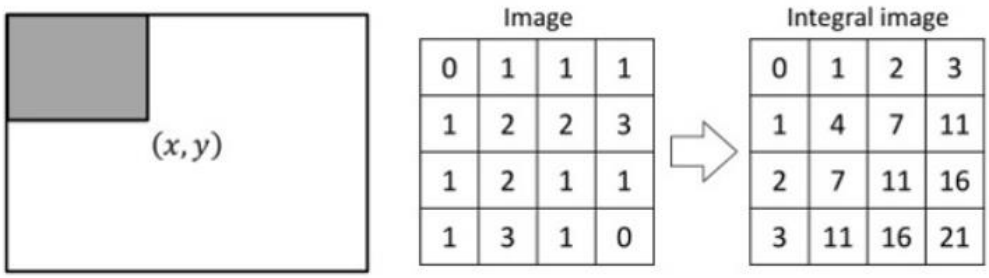

Рис. 2.16 Перетворення зображення в його інтегральне представлення

Для виконання задачі розпізнавання обличчя використовується так званий принцип скануючого вікна і виглядає наступним чином:

1. на вході є деяке зображення, яке представлено двовимірною матрицею пікселів розміром $w * h$, в якій кожен піксель дорівнює:

— від 0 до 255, якщо дано чорно-біле зображення;

— від 0 до 255^3 якщо дано кольорове зображення.

2. далі перед алгоритмом постає задача виділити всі знайдені обличчя, пошук відбувається в активній області спеціальними прямокутними признаками, за допомогою яких якраз таки і описується знайдене лице та його особливості:

$$rectangle_i = \{x, y, w, h, a\}, \tag{2.3}$$

де x, y — координати центру i-го прямокутника, w — ширина, h — висота та a — кут нахилу прямокутника до вертикальної осі зображення.

Особливості, які були використані Віолою та Джонсом, базуються на вейвлетах Хаара. Вейвлети Хаара представляють прямокутні хвилі однакової довжини (де один інтервал високий, а один низький). Прямокутна хвиля нагадує собою пару сусідніх прямокутників - один світлий і один темний.

Фактично прямокутні комбінації, які використовуються для візуального виявлення об'єкта, не є справжніми вейвлетами Хаара, а лише нагадують їх. Замість цього, ознаки Хаара містять прямокутні комбінації, які краще підходять для візуальних завдань розпізнавання.

Признаки Хаара представляють собою набір характеристик, які представляють результат порівняння яскравостей в двох різних прямокутних областях зображення. [8]

Припустимо, що існує множина об’єктів A та множина відповідей B. Нехай $g: A \to B$ називається вирішальною функцією. Вирішальна функція повинна допускати ефективну комп’ютерну реалізацію, тому її називають алгоритмом. Признак f об’єкта а є відображенням $f: A \to D_f$, де D_f — множина допустимих значень ознак.

Якщо задано набір ознак то вектор $x = f_1(a), \dots, f_n(a)$ називається ознаковим описом об'єкта $a \in A$. При цьому множина $A = D_{f1} \times \dots \times D_{fn}$ називається ознаковим простором.

В стандартному методі Віоли-Джонса використовуються прямокутні ознаки.

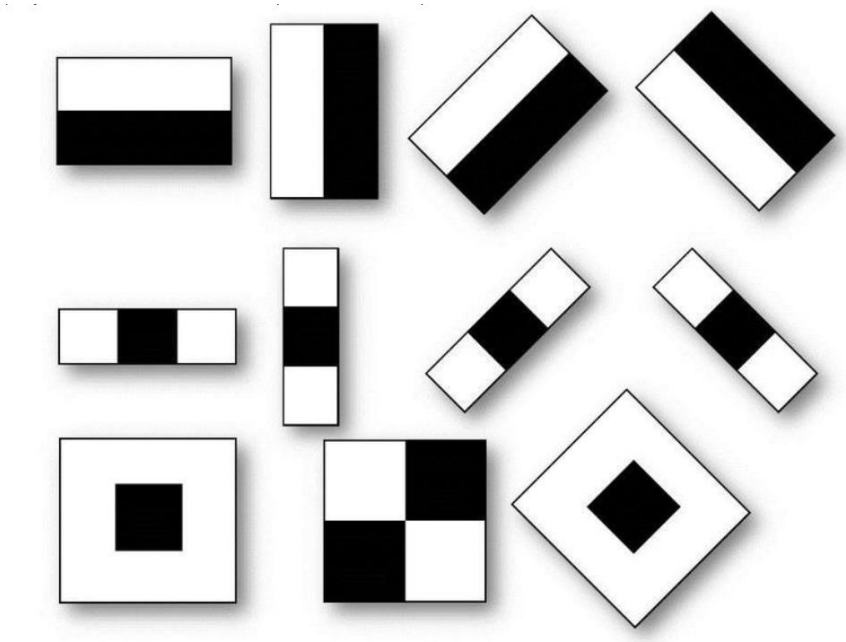

Рис. 2.17. Примітиви ознак Хаара

В розширеному методі Віоли-Джонса, який представлено в бібліотеці OpenCV, також використовуються додаткові ознаки.

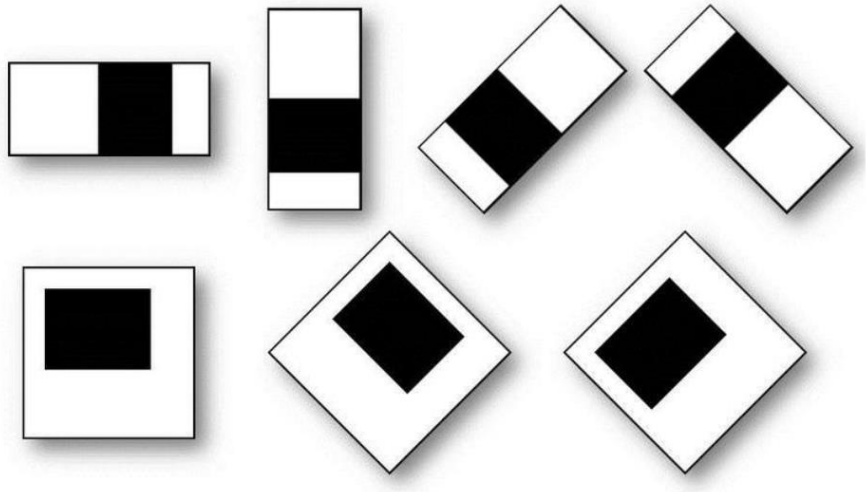

Рис. 2.18 Додаткові примітиви ознак Хаара з бібліотеки OpenCV

Обчислюваним значенням такого показника буде:

$$F = U - V, \tag{2.4}$$

де U — сума значень яскравості точок, що закриваються світлою частиною ознаки, а V — сума значень яскравості точок, що закриваються темною частиною ознаки. Для їх обчислення використовується поняття інтегрального зображення про яке говорилося вище. Ознаки Хаара описують значення перепаду яскравості по осях X та Y відповідно. [9]

В результаті сканування вікна за ознаками відбувається наступним чином:

1. на вхід подається досліджуване зображення, обирається вікно сканування, обираються використовувані ознаки;
2. далі обране вікно сканування починає послідовно рухатися по зображенню з кроком в 1 елемент вікна (припустимо, розмір самого вікна є 24 * 24 елементи);
3. в процесі сканування зображення в кожному вікні обчислюється більше ніж 200 000 різних варіантів розташування ознак, це відбувається за рахунок положення ознак в вікні сканування і зміни їх масштабу;
4. сканування проводиться раз за разом послідовно для різних масштабів, доки не будуть покриті всі можливі частини;

5. особливістю є те, що масштабується не саме зображення, а саме скануюче вікно;

6. всі знайдені ознаки потрапляють до класифікатора, де відбувається остаточне вирішення результату: зображення підходить або ні.

Для прискорення процесу виявлення облич використовується каскадний класифікатор, який фіксує роботу на найбільш цікавих ділянках зображення.

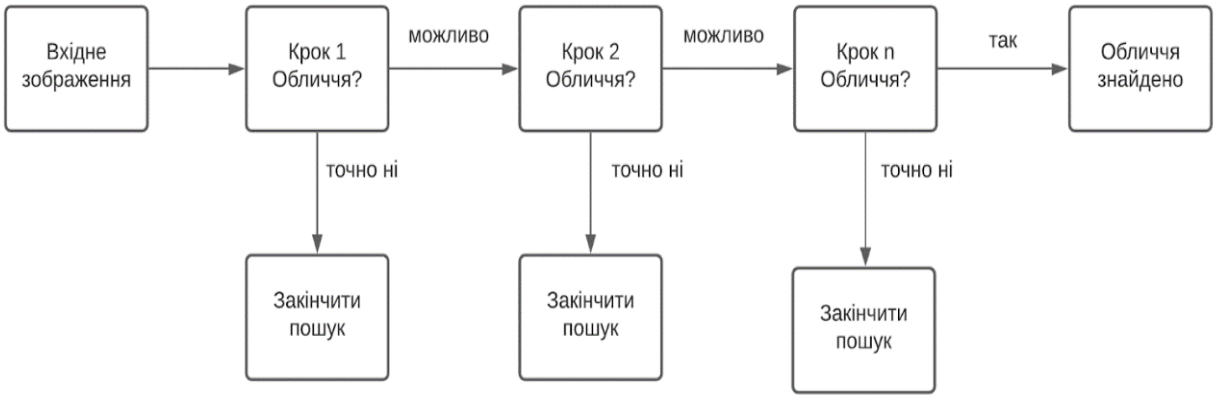

Рис. 2.19 Алгоритм роботи каскадного класифікатора

У даному розділі описано специфікацію систем контролю доступу, розглянуто кілька аналогів, які мають схожий функціонал.

Проаналізовано різні можливі підходи до виконання розпізнавання облич та виконано порівняння наведених підходів.

В результаті порівняння було вибрано розширений метод Віоли-Джонса через його високу ефективність та можливість роботи в реальному часі та наведено принцип роботи його алгоритму.

3. ЗАСОБИ РОЗРОБКИ ТА ОПИС ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

Кожна СКУД має чотири основних елементи (блоки):

— Ідентицікатор користувача(карта-перепустка, ключ, біометричні дані)

— Пристрій ідентифікації

— Керуючий контролер

— Виконавчий пристрій

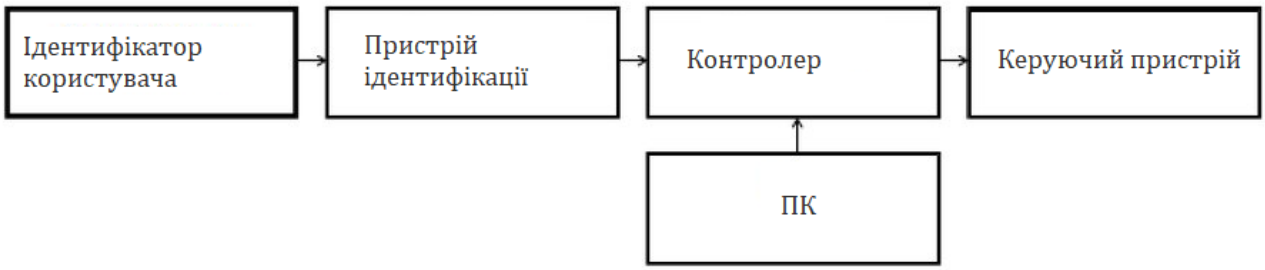

Рис. 3.1 - Узагальнена блок-схема систем безпеки

3.1 Структурна та функціональна схеми платформи

3.1.1 Структурна схема

Відповідно можна виділити наступні основні блоки системи та скласти структурну схему.

До основних блоків можна віднести:

1. Rasbperry Pi;
2. Модуль камери;
3. Дисплей;
4. Кнопки керування;
5. Н-міст;
6. Електромотор замка;
7. Джерело напруги;

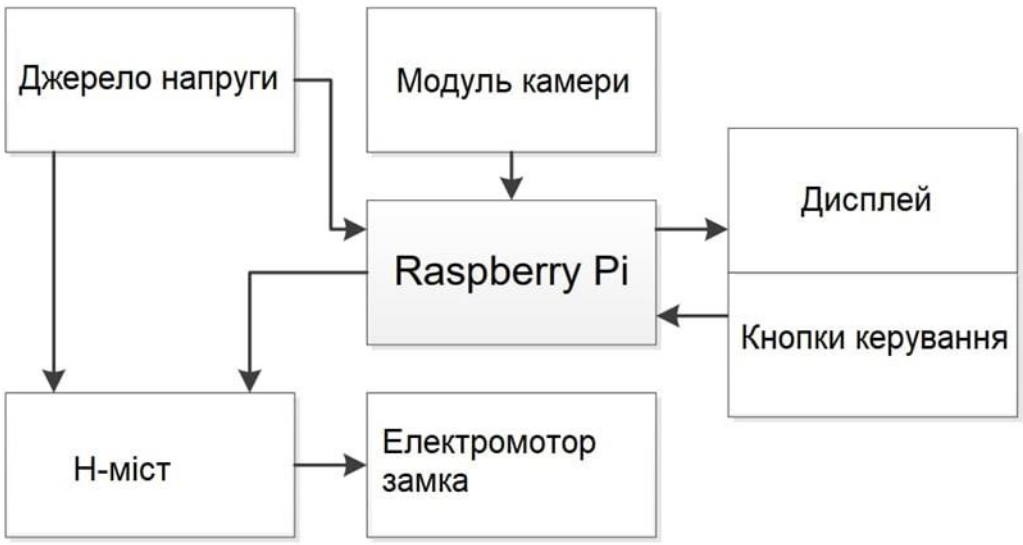

Рис.3.2. Структурна схема пристрою

Rasbperry Pi призначений для керування, контролю, аналізу та обробки та збереження даних, отриманих від камери , регулювання роботи підключених пристроїв, виведення даних на дисплей.

Кнопки керування необхідні для керуванням електромотором замка в ручному режимі.

Джерело напруги живить всю систему в реальному часі.

Дисплей може відображати результати для моніторингу роботи системи та відображення збережиних даних.

3.1.1 Зображення діаграми схема

Як можемо бачити в системі використовується кілька пристроїв з компонентами, а саме :

— мобільний пристрій та додаток запущений на ньому;

— пристрій Raspberry Pi та сервер з підключеною базою даних MySQL і компонент розпізнавання запущені на ньому;

— веб-камера;

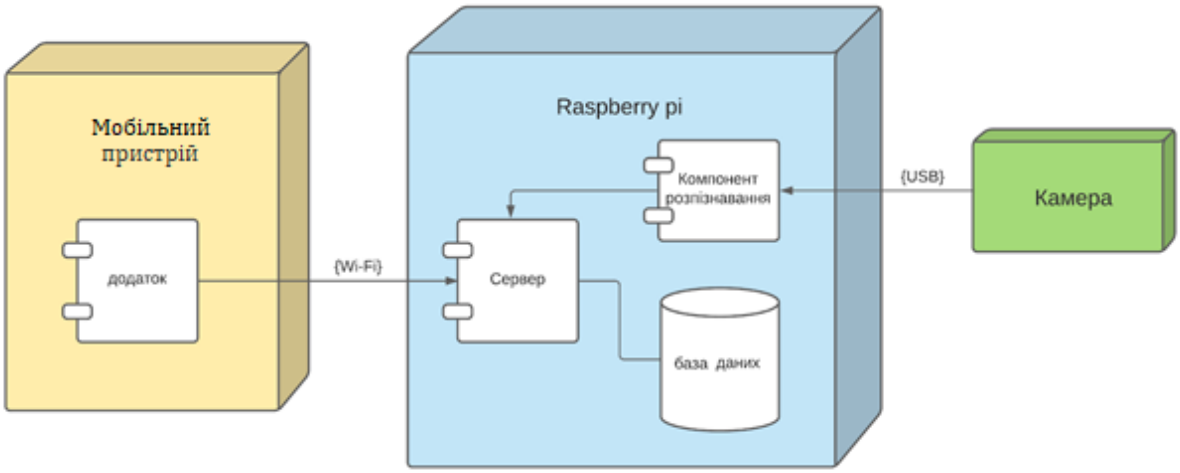

Рис. 3.3 Діаграма системи.

3.2 Обґрунтування та підбір комплектуючих

Апаратна частина складатися з декількох модулей, які будуть відповідати за певний функціонал та взаємодіяти між собою. Система складається із пристрою Raspberry Pi 4 Model B та звичайної веб-камери. Також було вирішено, застосовуючи GPIO та приєднати світлодіод, який буде світитися на протязі 3 секунд після фіксації обличчя зареєстрованої особи.

Також приєднано резистор для того, щоб не передавати надто великий струм по ланцюгу.

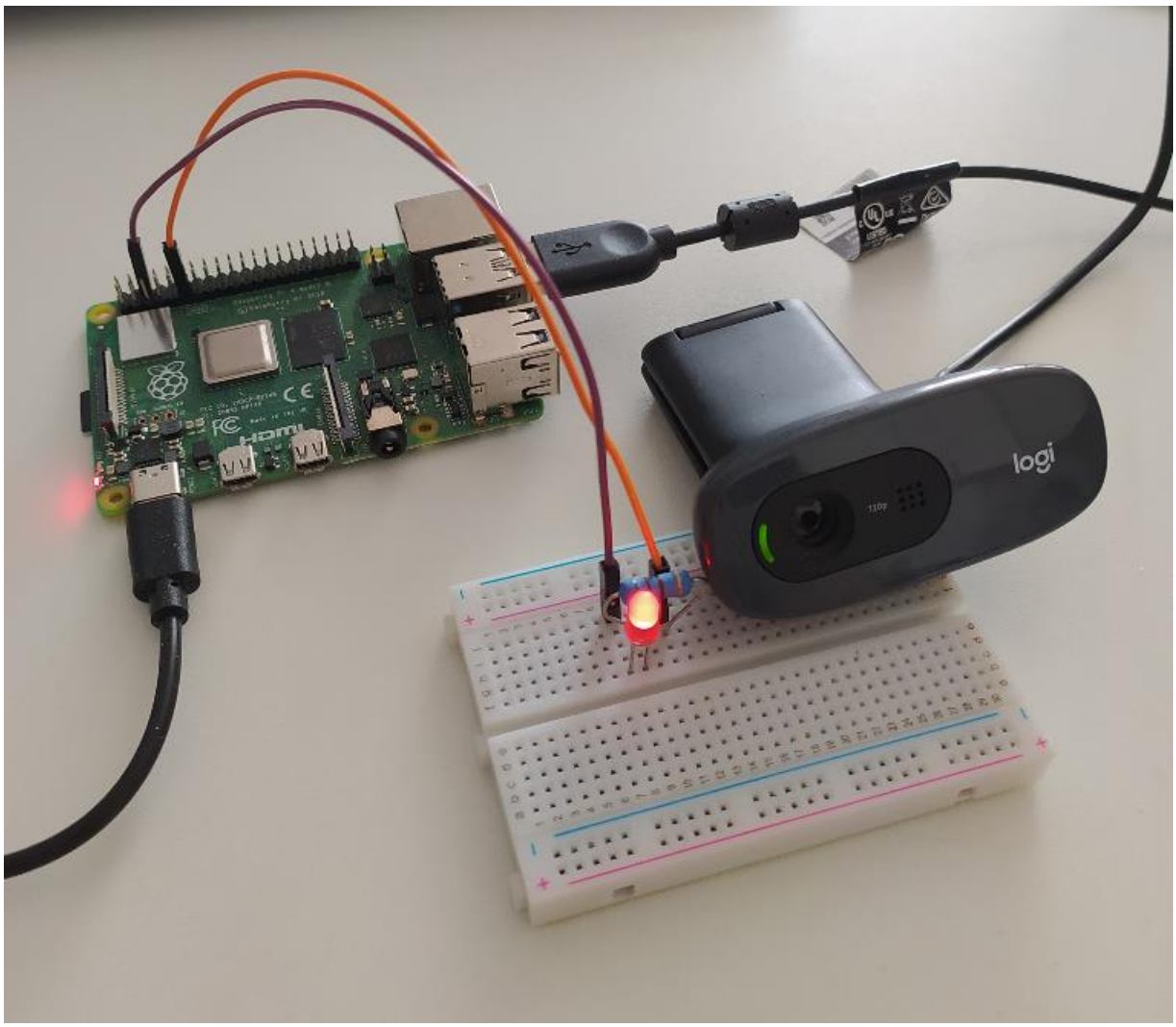

Рис. 3.4 Вигляд апаратної частини дипломної роботи

3.2.1 Raspberry Pi

Серія одноплатних комп’ютерів Raspberry Pi є надзвичайно популярною завдяки доступній ціні, зручному дизайну та компактним розмірам. Остання версія Raspberry Pi 4 Model B, яка використовується в даній дипломній роботі, є найпотужнішою на сьогоднішній день. Отримавши значне підвищення обчислювальної потужності та покращивши периферійне підключення, а також зберігаючи таку ж низьку ціну та мініатюрний розмір, модель є найкращим вибором для поставлених задач.

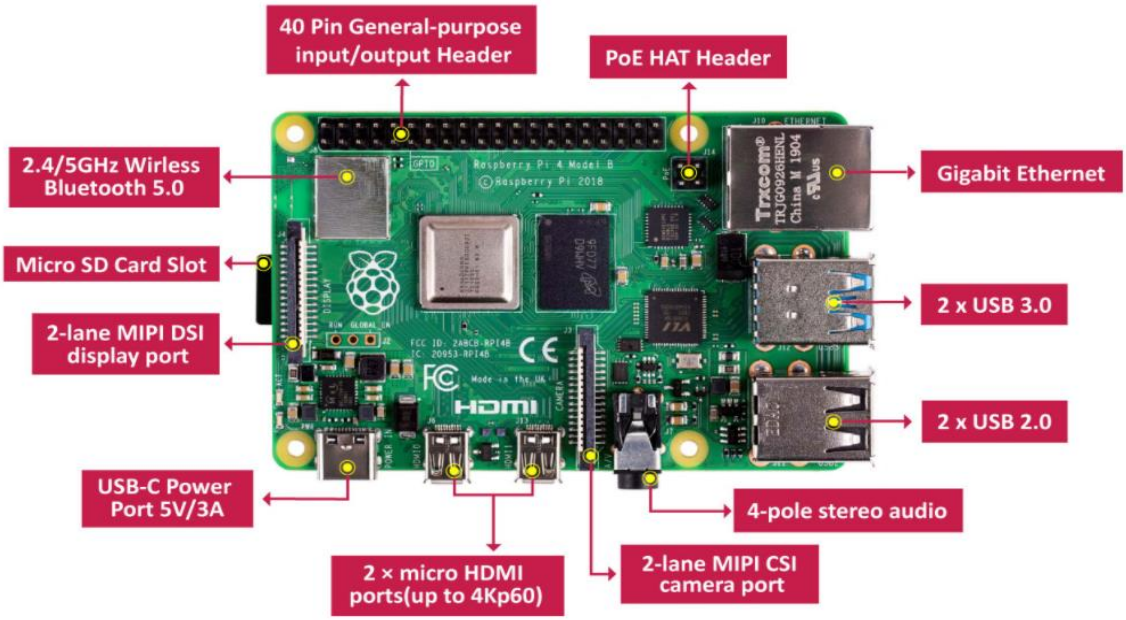

Рис. 3.5 Огляд Raspberry Pi 4 Model B

Новий Raspberry Pi 4, в порівнянні з попередніми версіями, отримав деякі оновлення, такі як порти USB 3.0, живлення через USB Type-C та Ethernet, а також вихід відеосигналу, що одночасно може працювати з двома моніторами 4K. Крім того, як і раніше, все ще модель підтримує всі можливості з'єднання та розширення штифтів GPIO Pi, а також сумісність із попередніми доповненнями та аксесуарами.

Можна виділити наступні переваги у використанні одноплатного комп'ютера Raspberry Pi 4 Model B:

— невисока вартість;

— достатньо велика потужність в компактній платі;

— Багато можливостей як для однієї плати (кілька USB, HDMI, Ethernet, вбудований Wi-Fi та Bluetooth, живлення через USB, багато GPIO, тощо);

— Підтримує Linux, Python (що полегшує створення додатків);

— доступні приклади роботи з пристроєм та створення невеликих систем за підтримки спільноти в мережі Інтернет;

Однією із особливостей Raspberry Pi 4 є роз'єм GPIO (рис 3.3.2), за допомогою якого можна підключати зовнішні пристрої.

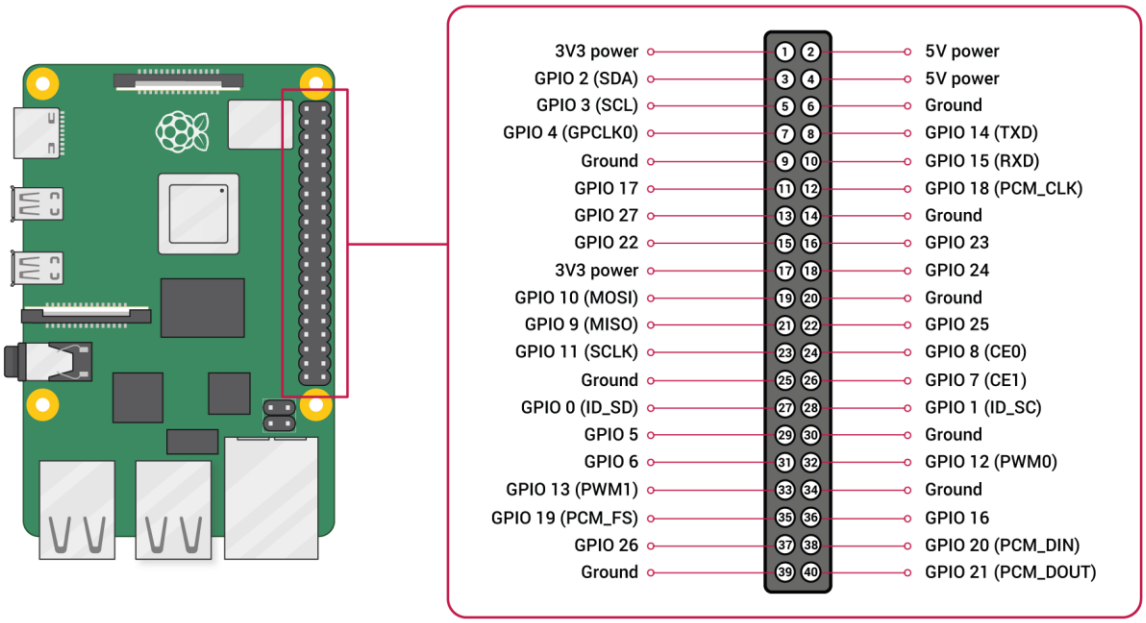

Рис. 3.6 Огляд GPIO пристрою Raspberry Pi 4

GPIO-роз'єм зазвичай складається з роз'ємів декількох різних типів:

— звичайні GPIO-виходи (інтерфейс вводу / виводу загального призначення), які можна використовувати, наприклад, для вмикання і вимикання світлодіодів і т. п.

— інтерфейсні виходи I2C, які дозволяють під'єднати модулі пристроїв за допомогою всього двох виходів;

— SPI-інтерфейс для SPI-пристроїв; схожий до I2C, але трохи інший стандарт;

— Послідовні Rx і Tx виходи для взаємодії з послідовними периферійними пристроями.

GPIO-роз’єми можуть бути використані як цифрові входи, так і цифрові виходи. У разі використання як цифрових виходів, можна писати програми, які зможуть задавати значення конкретного контакту як HIGH або LOW. HIGH задає значення 3,3 В, а LOW — 0В. Щоб керувати світлодіодом через один з

GPIO, знадобиться резистор на 1кОм послідовно приєднаний до світлодіоду, оскільки контакти GPIO можуть витримувати тільки невеликі кількості струму.

Для виконання роботи на пристрій було встановлено OS Raspbian, яка є ідеальним дистрибутивом для Raspberry Pi будь-якої моделі, оскільки при виході нових версій одноплатних комп'ютерів ця операційна система отримує оновлення в першу чергу. До того ж Raspbian спеціально оптимізована для роботи на низькопродуктивному процессорі ARM, що використовується серії Raspberry Pi.

3.2.3 Інші комплектуючі системи

Також було вирішено, застосовуючи GPIO та приєднати світлодіод, який буде світитися на протязі 3 секунд після фіксації обличчя зареєстрованої особи.

Також приєднано резистор для того, щоб не передавати надто великий струм по ланцюгу.

Оскільки основною задачею було створити бази для подальшої роботи, у даній схемі було замінено механізм відкривання дверей, на світлодіод, який вказує на сигнал, що подається на механізм відкривання дверей. Світлодіод світиться — двері відкриті.

Якщо говорити про розпізнавання облич, то зареєстрованій людині, яка намагається пройти через пункт розпізнавання достатньо подивитися в камеру на проміжок часу менше однієї секунди.

Варто сказати, що алгоритм розпізнавання також дозволяє і фіксувати обличчя під невеликим кутом до 30 градусів.

Рекомендована відстань розпізнавання розробленої системи — від 0.5 метра до 2 метрів.

Для роботи пристрою необхідне постійне джерело струму, також є можливим використання батарейних блоків, як повноцінне джерело струму, або як запасний варіант у випадку зникнення підключення до електромережі.

3.2 Моделювання

Схему перевірено на роботу у середовищі Proteus 8.

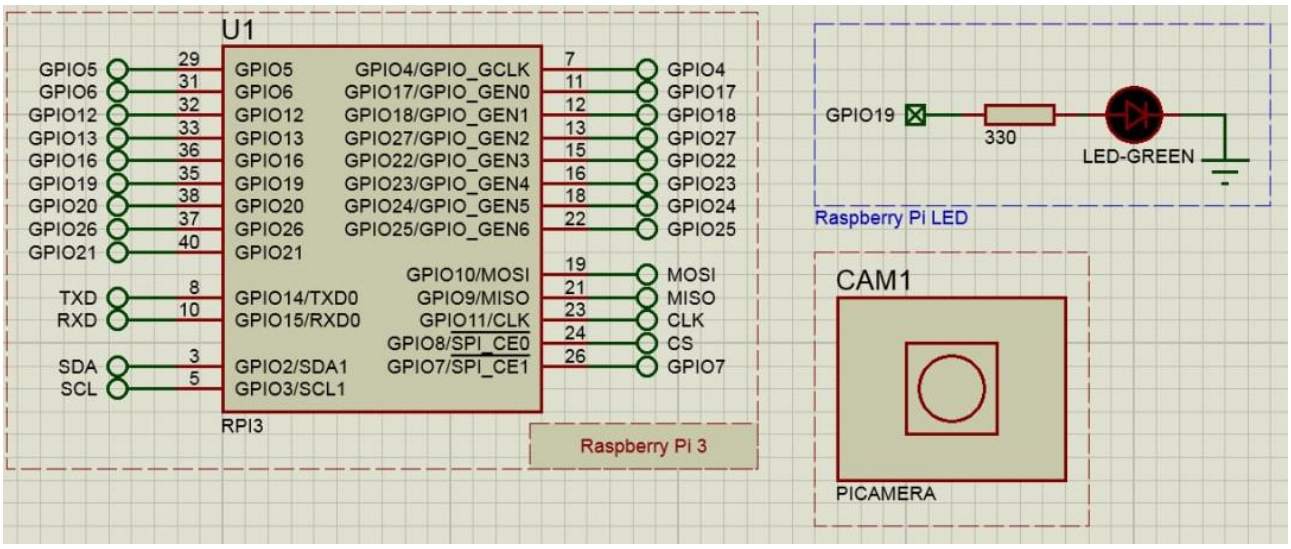

Рис. 3.7 Схема моделювання на середовищі Proteus 8

3.3 Опис розпізнавання обличчя

Алгоритм складається з двох різних процесів: виявлення(збереження) ознак відомих осіб в базі даних та розпізнавання облич.

При виявленні обличчя (виявляється лише обличчя людини), програмне забезпечення не матиме уявлення про те, хто ця особа. У програмі «Розпізнавання обличчя» програмне забезпечення не тільки розпізнає обличчя, але й розпізнає людину. Тепер повинно бути зрозуміло, що перед виконанням розпізнавання обличчя нам потрібно виконати функцію «Визначення обличчя».

Процес збереження ознак відомих осіб відбувається наступним чином:

1. Перетворення зображення відео фрейма в півтонове зображення.
2. Застосування до напівтонового зображення методу Харра для пошуку ділянок обличчя.
3. Зменшення розміру області особи до 64 × 64 пікселів.

4. Застосування до отриманого на кроці 3-х зображень перетворення для отримання ознак особи (вейвлет коефіцієнтів).

5. Збереження витягнутих ознак в базі даних.

У процесі розпізнавання невідомої особи здійснюються кроки 1-4, потім на основі застосування методу головних компонент відбувається зі припиненням числа ознак і їх порівняння з рисам, що зберігаються в базі даних.

Опис алгоритму роботи всієї системи:

1. Тренувальний процес: ми підготували кілька образів відомі особи в базі даних. На час навчання збираємо максимальну кількість зображень людини.

Чим більше кількість зразків, тим більше буде точність системи.

2. Процес розпізнавання: Як тільки відвідувач натискає дверний дзвінок, камера робить знімок і намагається відповідати збереженій в ньому базі даних. Якщо збіг знайдено, тоді він надсилає фото в телеграм.

Надання дозволу: Після отримання фото, порівнюється інформація, і здійснюється вибір щодо доступу.

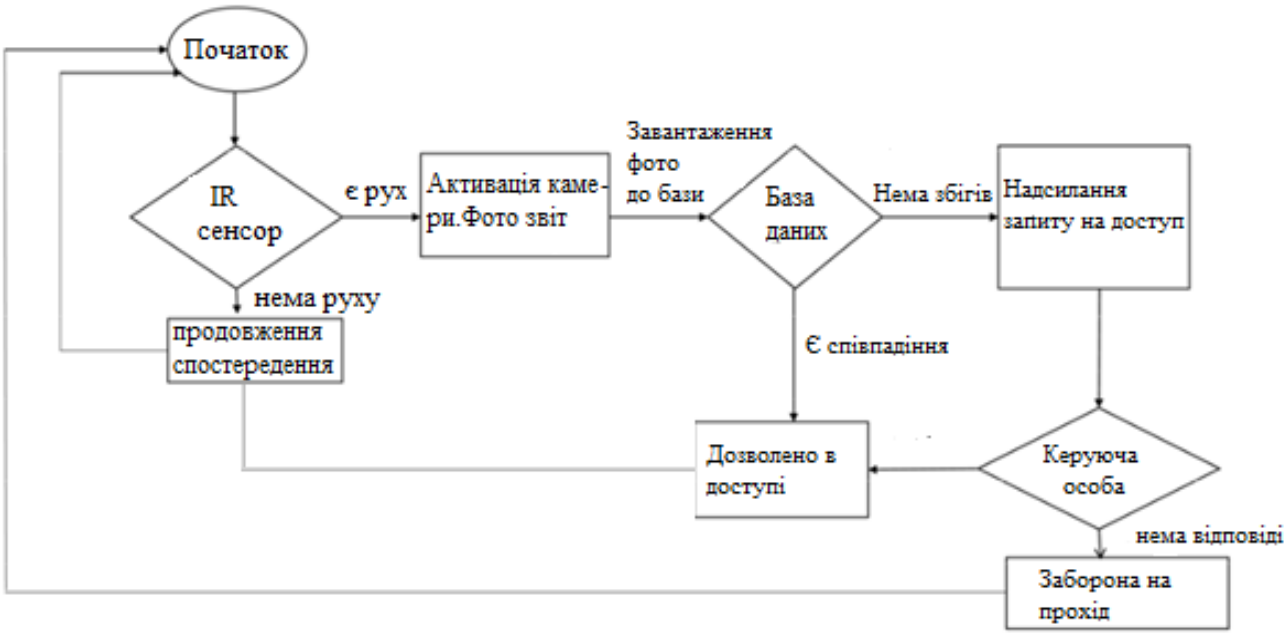

Рис.3.8 Алгоритм роботи

Основне призначення системи доступу - це надання повноважень відповідно до існуючих даних.

Система є автоматичною, коли робота відбувається з людьми що є в базі даних. При виявлення невідомих відбувається запит до керівника, адміністратора.

Задачею оператора або адміністратора можуть бути облік та обробка зібраної системою контролю доступу інформації, такої як особисті дані користувачів, фото, часу фіксувань осіб чи транспорту на пункті пропуску.

Також до повноважень можна віднести реєстрацію та надання рівню доступу, видачу нових перепусток, контролю стану роботи різних пристроїв системи. У випадку великої кількості виконуваних функцій часто наймаються кілька працівників, які розподілено між собою виконують описані задачі.

3.4 Опис програмної реалізації сервера

Rest сервер, написаний за допомогою мови програмування python, представляє центральний компонент системи з яким спілкуються всі інші елементи системи: компонент розпізнавання та мобільний додаток.

Саме на сервері відбуваються передача даних до бази даних та передача по запиту даних з бази даних, яка як і сервер знаходиться в пристрої Raspberry Pi. Основною причиною того що ці компоненти знаходяться на одному пристрої є поставлена задача розробити автономну систему яка не залежить від підключення до мережі Інтернет.

Основною частиною сервера є REST controller, де прописані всі можливі URL шляхи по яким можна подавати запити. За допомогою такої побудови ми маємо можливість звертатися до бази даних використовуючи GET, POST, DELETE запити та ін. Відповіді відправляються у вигляді JSON формату.

Наведемо основний реалізований набір можливих запитів до сервера через шлях URL в локальній мережі:

— GET запити для повернення всіх користувачів чи одного конкретного;

— GET запити для повернення історії фіксувань чи одного конкретного запису по користувачу;

— POST запит для створення нової помітки часу фіксування;

— POST запит для створення нового користувача;

— DELETE запит для видалення користувача.

Також варто зауважити, що сервер розроблений таким чином, що у випадку повного виконання запиту буде відправлена відповідь компоненту про корректне спрацювання, а саме код 200.

У випадку ж коли запит не відбувся через певні причини буде повернутий код помилки, наприклад, код 403 (сервер не відповідає), або 501 (метод не розпізнає метод запиту або не вдається його виконати).

Саме на сервері відбувається з'єднання з базою даних MySQL, для цього в коді введено конфігураційні дані зображені на рисунку 4.4, які включають логін, пароль, назву бази даних та ін.

```
import mysql.connector as mariadb

config = {
    'host': '127.0.0.1',
    'port': 3306,
    'user': 'root',
    'password': 'root',
    'database': 'face_recognition'
}
```

Рис. 3.9. Інформаційна структура системи.

3.5 Розробка програмного забезпечення

Для розпізнавання осіб на Raspberry Pi були встановлені пакети OpenCV, face_recognition і imutils, щоб навчати нашу платформу на основі зображень, використовуваних як датасет.

OpenCV – це бібліотека алгоритмів з відкритим вихідним кодом для обробки зображень та відео.

Пакет Python face_recognition застосовується для порівняння зображень обличчя в наборі даних.

Imutils - це серія зручних функцій для прискорення вичислення OpenCV на Raspberry Pi.

Файл headshots.py необхідний для реєстрації адміністратором нової людини, яку буде пропускати система, для цього необхідно запустити файл та вказати унікальне ім’я людини, яку необхідно зареєструвати, а також створити папку з таким же ім’ям в папці dataset, як це зображено нижче. Далі ввімкнеться камера і сфотографує людину, яку намагаємося зареєструвати. Фото треба робити з різних ракурсів обличчя для кращого розпізнавання людини.

Файл train_model.py відповідає за аналізу зображень в датасеті. У результаті створюємо відповідність між іменами та особами в файлі encodings.pickle.

Датасет: train_model.py аналізує фото в папці dataset. Розбито знімки по іменах.

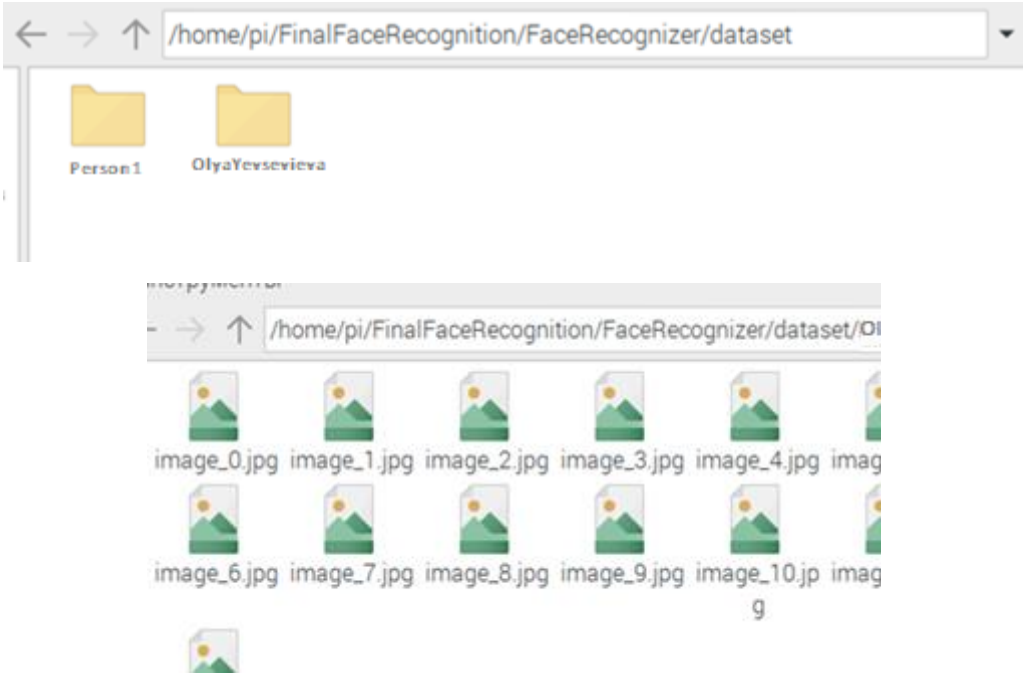

Рис. 3.10 Зображення роботи “train_model.py

По завершенні навчання Pi, запустимо facial_req.py для ідентифікації осіб та побачимо результат.

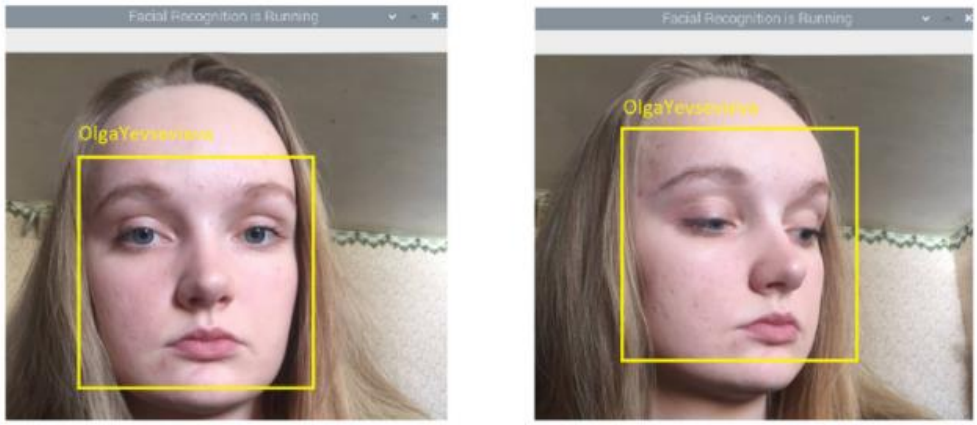

Рис. 3.11 Розпізнавання обличчя

Всі люди, які фіксуються камерою розпізнаються і порівнюються з зареєстрованими користувачами, якщо дана людина є зареєстрованою то сигнал про це йде на основний сервер і дані про час та ім’я фіксуються в базі даних.

Сервер, написаний за допомогою фреймворку flask мови програмування python, формує центральний компонент системи, з яким спілкуються компоненти розпізнавання та мобільний додаток. Саме на сервері відбуваються передача даних до бази даних MySQL та передача по запиту даних з бази даних, яка як і сервер також знаходиться в пристрої raspberry pi.

Основною причиною того що ці компоненти знаходяться на одному пристрої є поставлена задача розробити автономну систему, яка не залежить від підключення до мережі Інтернет. Сервер запускається для локальної мережі в консолі, де ми можемо побачити всі запити які проходять через сервер, як зображено нижче.

```
192.168.0.101 - - [16/June/2021 10:12:59] "Get /personal HTTP/1.1."200 -
192.168.0.101 - - [16/June/2021 10:12:59] "Get /story HTTP/1.1" 200 -
192.168.0.101 - - [16/June/2021 10:12:59] "Get /persons HTTP/1.1" 200 -
192.168.0.101 - - [16/June/2021 10:12:59] "Get /story/name?name=OlyaYevsevieva HTTP/1.1" 200 -
```

Рис. 3.12 Зображення запуску сервера

Через те, що детектування особи в кадрі відбувається за допомогою примітивів Хаара, програма не «втрачає» особу в кадрі, навіть якщо закрити нижню частину обличчя або закрити лоб. Однак, як тільки будуть закриті очі

або ніс, то особа «губиться» програмою - не відбувається ідентифікація особистості.

В ході проведення експериментальних досліджень на обмеженій вибірці осіб (наприклад, доступ до кімнати) було виявлено, що система розпізнає обличчя людини з ймовірністю близько 90%. Для повноцінної оцінки системи потрібно налаштування і перевірка її на реальному об'єкті.

Перевагою запропонованого рішення є її реалізація на платформі Raspberry Pi, яка володіє малою потужністю і низькою вартістю. недоліки цієї платформи (малий обсяг пам'яті і низька швидкодія) не є для даної системи критичними, так як її можна легко модернізувати відповідно до вимог замовника, наприклад, використовувати більш потужну платформу Raspberry Pi 4B. До платформи також можливе підключення відеокамери з ІЧ-підсвічуванням для усунення такого недоліку в роботі як відсутність достатнього рівня освітленості, властивого оптичним системам.

Для високого рівня безпеки в цій пропозиції використовуються дві нові технології Інтернет речей і обробка зображень. Пропонована робота реалізується з використанням плати Raspberry pi, яка може бути інтерфейсом на мобільному додатку або ПК, отже, користувач може керувати системою легко. Запропонована система є комплексним рішенням всіх існуючих робіт, в яких ІЧ-сенсор використовується для виявлення об'єктів, які по черзі запускають камеру для розпізнавання облич.

Система призначена для віддаленого доступу та управління розумним приміщенням.

4. РОЗРОБКА НАВЧАЛЬНОГО СТЕНДУ

4.1 Загальна схема підключення

Основний принцип роботи: контролер обробляє інформацію, що надходить з зчитувача, і за допомогою вбудованого реле комутує виконавчий пристрій – замок на дверях.

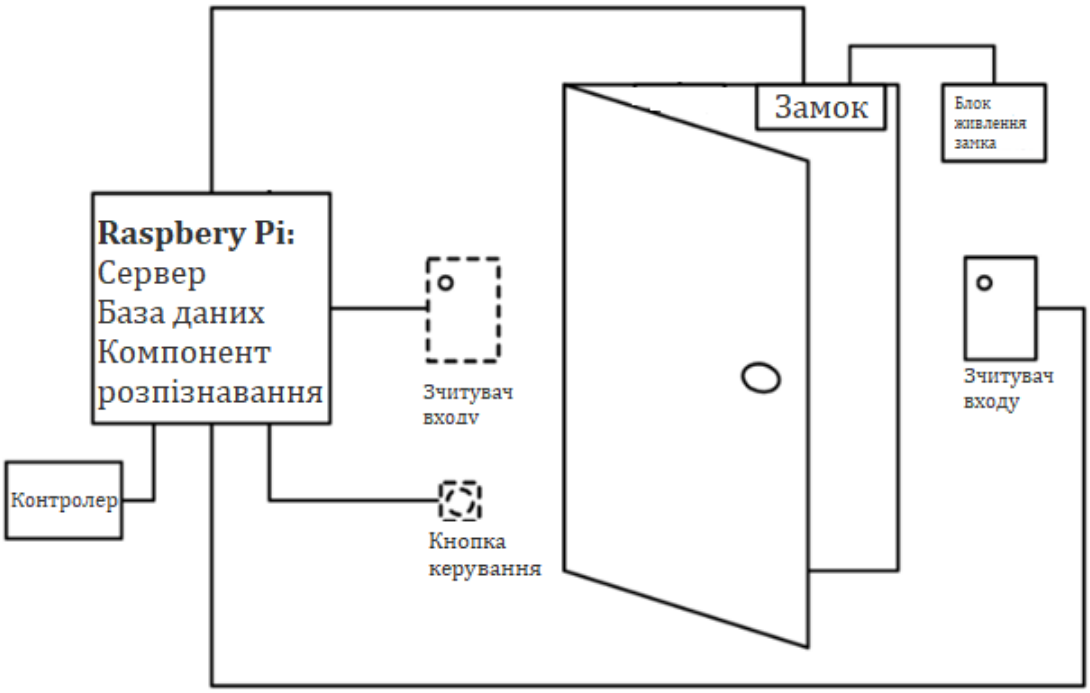

Рис. 4.1. Схема підключення системи

4.2 Створення мобільного додатку

Мобільний додаток написаний за допомогою фреймворку Flutter та мови програмування Dart надає простий і зручний спосіб спілкування з сервером.

Структура проекту з мобільним додатком є характерною для використання фреймворку Flutter та налічує безліч файлів, необхідних для можливості запуску додатку на різних платформах. Далі розглядатимемо саме мобільну Android платформу.

У папці lib знаходиться основний написаний код, а інші є частиною стандарно згенерованого Flutter додатку.

Структуру проекту мобільного додатку, який представляє інтерфейс для спілкування з сервером, зображено на рисунку 4.9.

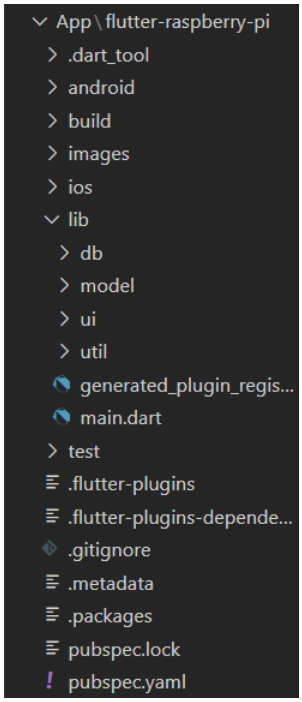

Рис. 4.2. Структура Flutter додатку

UI додатку створюється за допомогою набору класів, що імпортуються зі стандартного набору бібліотек фреймворку та представляють деревовидну структуру.

Для зручності користування мобільним додатком було створено спеціальне меню знизу екрану з можливістю перемикання між функціональними можливостями програми.

Додаток побудовано таким чином щоб звертатися до сервера за допомогою запитів у випадку якщо телефон та Raspberry Pi знаходяться на даний момент в одній локальній мережі. У результаті отримуються дані у JSON форматі, обробляються та виводяться на екран.

JSON формат обрано через його простоту у використанні та наявність бібліотек для обробки таких даних.

Дані, що виводяться на екран відсортовано ще на рівні запиту до бази даних для якомога швидшого виводу даних. А саме:

— користувачі відсортовані за алфавітом;

— історія фіксувань відсортована за часом, щоб була змога переглядати останні зміни.

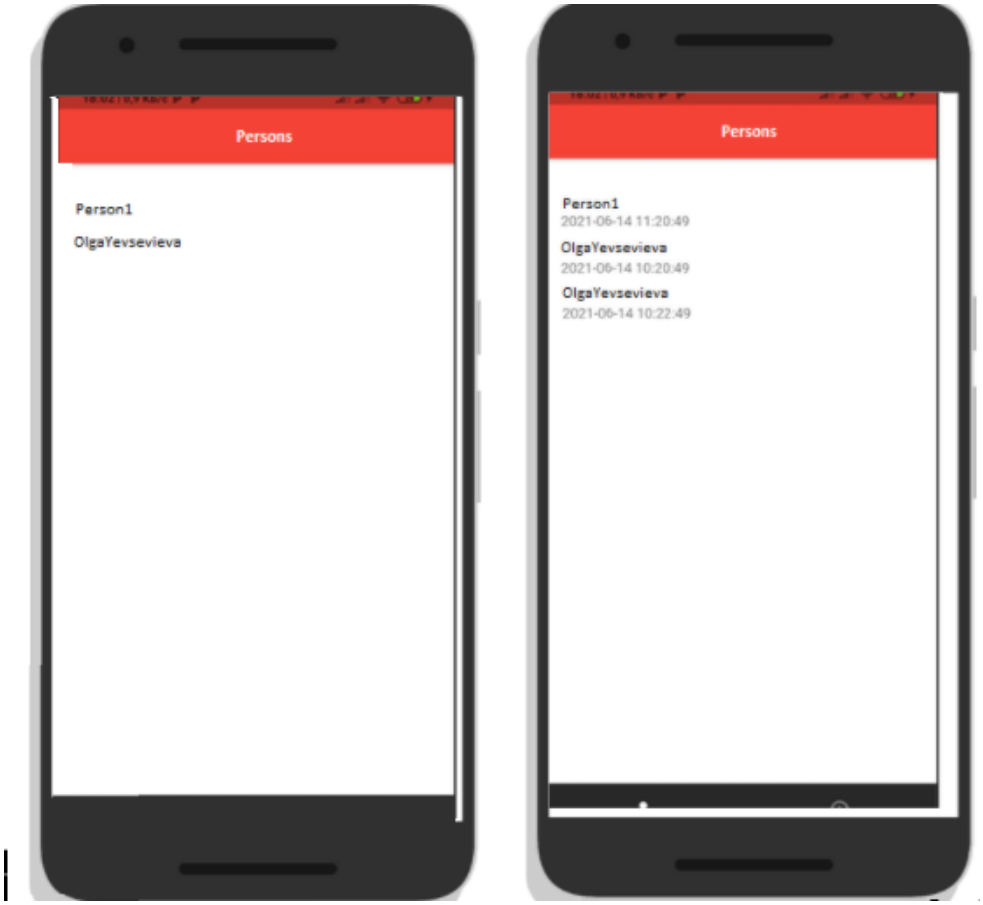

Рис. 4.3 Вигляд мобільного додатку

ВИСНОВКИ

Існуючі в даний час СКУД занадто спеціалізовані та підв'язані під цілий комплекс інших завдань та функцій, а налаштування є залежними від постачальника\виробника, вимагають постійної абонплати використовуваних ресурсів та оновлення, і при цьому жодна з них не гарантують 100% безпеку.

Тому розроблено систему, яка комплексно вирішує завдання швидкого встановлення та розгортання, зрозумілим інтерфейсом користувача та індивідуальними налаштуваннями для підвищення рівня безпеки.

За результатами аналізу існуючих систем контролю доступу розроблена система керування, що дозволяє не лише керувати ним, а відображати дані у мобільному додатку, в режимі реального часу. Розроблена система має функцію розпізнавання користувача, що дасть змогу покращити захист інформації. Було розроблено додаток, що має наступні властивості:

- дозволяє переглядати історію фіксувань зареєстрованих людей камерою;
- дозволяє переглядати список зареєстрованих користувачів;
- дозволяє переглядати історію фіксувань по кожному зареєстрованому користувачу окремо.

Виконано всі необхідні етапи і поставлені на початку задачі, а саме:

— провденно огляд існуючих автоматизованих систем контролю дступом.
— запропоновано схему реалізації автономного СКУД;
— розроблено структурну, функціональну схему системи з підбором та обґрунтуванням комплектуючих ;
— розроблено програмне забезпечення для системи технічного зору.
— отримано експериментальні дані ефективності запропонованого рішення.
— розроблено мобільний додаток для перегляду зафіксованої системою інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондаренко О. В., Карпінець В. В. Двофакторна аутентифікація в системах контролю і управління доступом. *Молодь в науці: дослідження, проблеми, перспективи,* 2020.URL: https://conferences.vntu.edu.ua/index.php/mn/mn2020/paper/view/10276.].
2. Резанов Б. М., Бульба С. С., Шокотько Д. В. Фактори аутентифікації системи контролю та управління доступом. *Системи управління, навігації та зв'язку.* 2017. Вип. 3 (43). С. 63-65.
3. СКУД – система контроля и управления доступом. 2021. URL: https://smarthomegadget.ru/skud-sistema-kontrolya-i-upravleniya-dostupom/ (дата звернення: 31.05.2021).
4. Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации, 2010. 58-61, 107-112 с.
5. Ворона В.А., Тихонов В. А. Системы контроля и управления доступом. Москва: Горячая линия – Телеком, 2010. 10-53 с.
6. Прохоренок Н. А. OpenCV и Java. Обработка изображений и компьютерное зрение / Санкт-Петербург: БХВ-Петербург, 2018. 13–46 с.
7. He K., Zhang X., Ren S., Sun J., Deep Residual Learning for Image Recognition. Conference on Computer Vision and Pattern Recognition. 2015. 26-28 pp.
8. Shapiro L. G., Stockman G. C. Computer Vision. Prentice Hall, 2001. 603. 615 с.
9. Гонсалес Р., Вудс. Р Цифровая обработка зображений. Москва: Техносфера, 2005. 1070 с.
10. Распознавание лиц на основе OpenCV для C++ (Facial Recognition based on OpenCV C++). 2018. URL: https://api-2d3d-cad.com/face_recognition_with_opencv/ (дата звернення: 31.05.2021).

ДОДАТОК Г

S U M M A R Y

Autonomous room access control system

The diploma project of first educational level "Bachelor" by specialty 171 Electronics, specialization ELECTRONIC DEVICES AND EQUIPMENT Yevsevieva Olga. National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute». Faculty of Electronics, Department of Electronic Devices and Systems. Academic group DE-71. - Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2021. - 53 p., Ill. 34.

INTRODUCTION

Access control and management systems (ACMS) are an important part of security systems today. They allow you to restrict, streamline access control to different rooms, while recording information about the movement of people for further use.

ACS is not just hardware and software, it is a fully designed system that can identify people, control access, store and analyze the data obtained.

Access control is the selective restriction of access to a specific place, room, resource, or institution. To gain access to a restricted location, an individual must usually be authorized or logged in.

The current ACSs are too specialized and tied to a whole range of other tasks and functions, and the settings depend on the supplier / manufacturer, require constant subscription fees and updates, and none of them guarantee 100% security.

Therefore, there is a problem of developing a system that would comprehensively solve the problem of quick installation and deployment, clear user interface and individual settings to increase security.

The purpose of the work is to develop an effective system of access control and management based on a system of technical vision using facial recognition algorithms. The research method is experimental.

An additional feature of this system will be to allow the user to use the interface to view the result of the work.

The list of the main tasks to be implemented in this system:

- visual identification;
- formation of individual and group access powers;
- access control through the interface;
- time accounting.

In this work, the aim is to create an autonomous control system for access to the premises, which implements the above tasks. Also, this system does not require additional tools to interact with the user.

DEVELOPED DEVICE

The system will consist of several modules that will respond to a certain functionality and interaction with each other.

Accordingly, you can select the following main blocks of blocks and make a block diagram.

1. Rasbperry Pi;
2. Camera module;
3. Display;
4. Control buttons;
5. H-bridge;
6. Electric motor of the lock;
7. Voltage source;

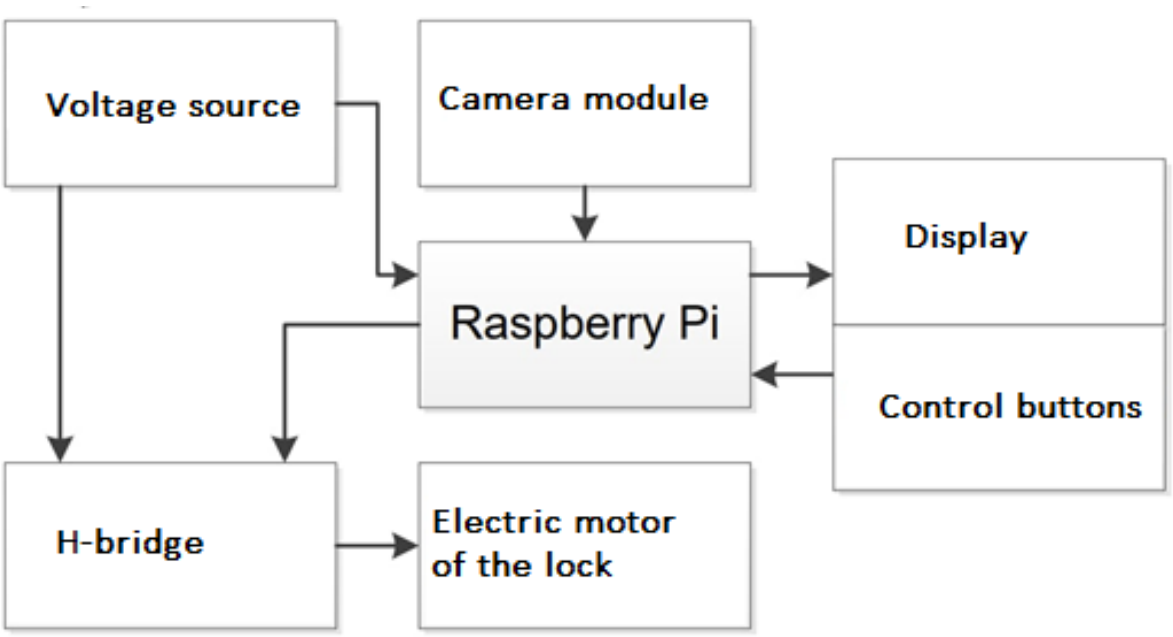

Fig. 1 Block diagram of the device

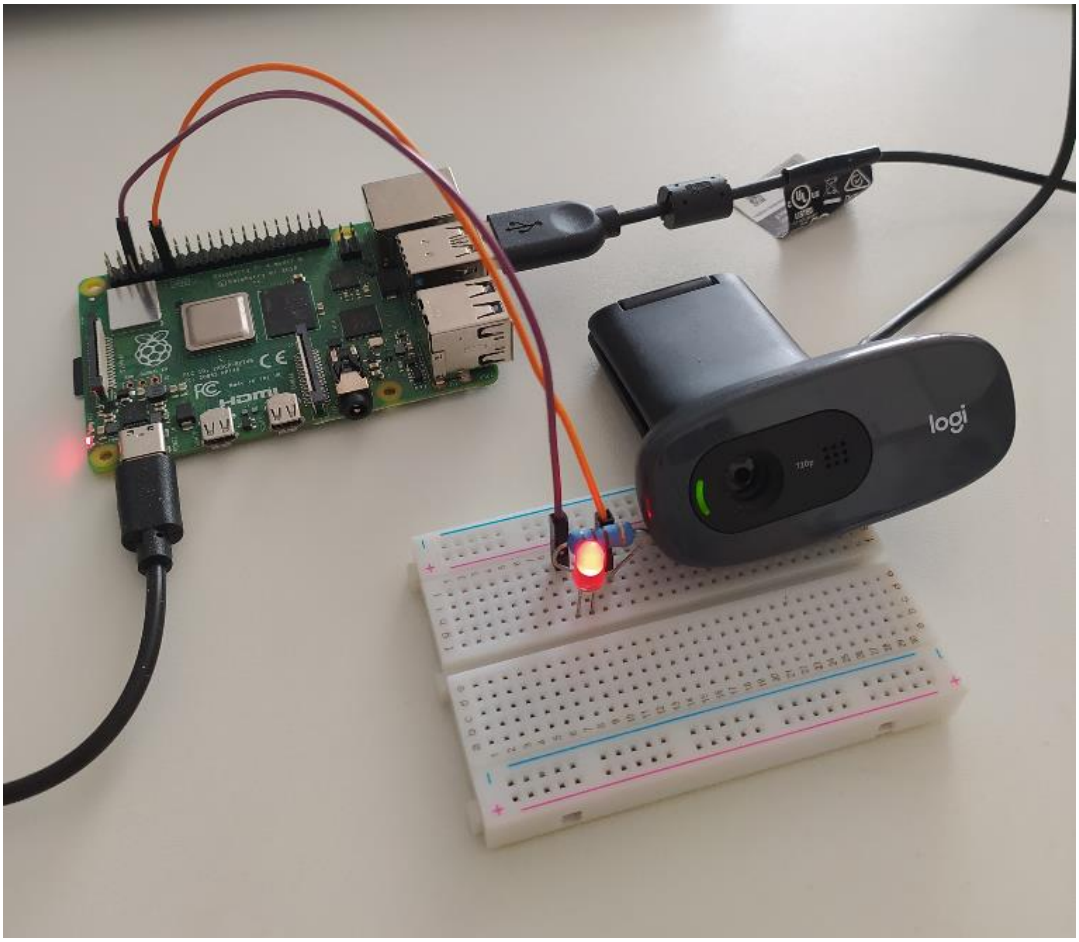

Fig. 2 View of the hardware of the system

ALGORITHM OF WORK

The algorithm consists of two different processes: detection (preservation) of features of familiar people in the database and face recognition.

When a face is detected, only the person's face is detected, the software will have no idea who that person is. In Face Detection, software not only recognizes faces, but also recognizes people. It should now be clear that we need to perform the Face Detection function before performing face recognition.

The process of preserving the features of famous people is as follows:

1. Convert a video frame image to a halftone image.
2. Apply the Harr method to the halftone image to find the area of the face.
3. Reduce the size of the face area to 64 × 64 pixels.
4. Application to the transformation obtained in step 3 of the image to obtain facial features (wavelet coefficients).
5. Saving extracted features in the database.

In the process of recognizing an unknown person, steps 1-4 are performed, then based on the application of the principal components method, the number of features ceases and they are compared with the features stored in the database.

Description of the algorithm of the whole system:

1. Training process: we have prepared several images of famous people in the database. At the time of training, we collect the maximum number of images of a person. The greater the number of samples, the greater the accuracy of the system.
2. Recognition process: As soon as the visitor presses the correct call, the camera takes a picture and tries to match the database stored in it. If a match is found, then he sends the photo in a telegram.
3. Granting permission: After receiving the photo, the information is compared, and a choice is made regarding access.

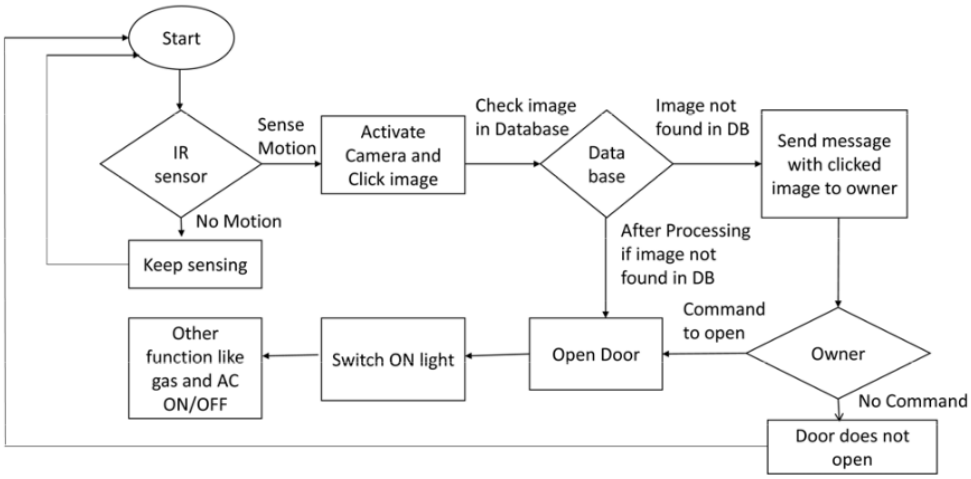

Fig. 3 System operation algorithm

All people who are recorded by the camera are recognized and compared with registered users, if this person is registered, the signal goes to the main server and the time and name data are recorded in the database.

The server is the central component of the system with which the recognition components and the mobile application communicate. It is on the server that data is transferred to the database and on request data is transferred from the database, which, like the server, is also located in the raspberry pi device.

The main reason that these components are on the same device is the task of developing a stand-alone system that does not depend on the Internet connection. Face recognition in the frame is done using the Haar method, will not detect error, even when closed some parts of the forehead or chin. But in the absence of eyes or nose in the frame, recognition becomes impossible. The advantage of the proposed solution is its implementation on the Raspberry Pi platform, which is powerful and compact. The disadvantages of this platform are low memory and low speed.

These shortcomings are not critical to this. For a high level of security, this offer uses two new Internet of Things technologies and image processing. This work is implemented using a Raspberry pi card, which can be an interface on a mobile application or PC. The user can operate the system easily. The system is designed for remote access and control of a smart room.

RESULTS OF WORK

As a result, Existing control systems are analyzed. A access control system has been developed that allows not only to manage it, but also to display data in a mobile application in real time. The developed system has a user recognition function that will improve information security. An application written using the Flutter framework and the Dart programming language has been developed with the following features:

- allows you to view the history of recordings of registered people by the camera;
- allows you to view the list of registered users;
- allows you to view the history of fixations for each registered user separately.

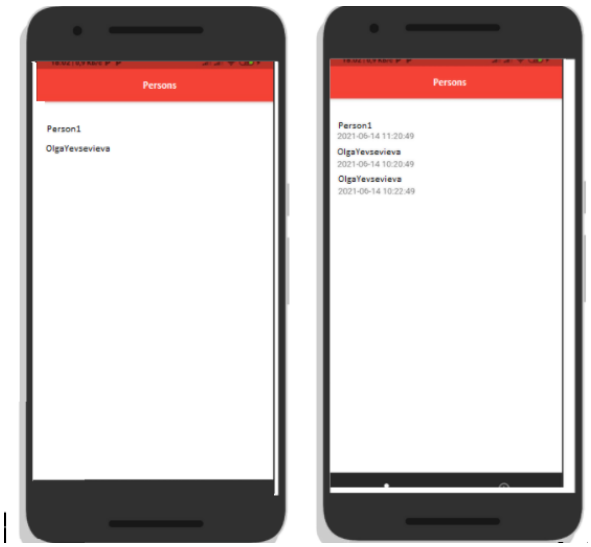

Fig. 4 Appearance of the web application

The data displayed on the screen is sorted at the level of the query to the database for the fastest possible output. Namely:

- users are sorted alphabetically;
- Lock history is sorted by time to be able to view recent changes.

Keywords: access control system, Raspberry Pi, face recognition.