Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
Охорона (назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Методи та засоби автоматичного розпізнавання відвідувачів в домофонних системах

Виконав: студент 6 курсу групи СІм-61 ,
спеціальності 123 «Комп’ютерна інженерія»
(шифр і назва спеціальності (напряму підготовки))

	(підпис)	Шевчук Ю.В. (прізвище та ініціали)
Керівник	(підпис)	Стадник Н.Б. (прізвище та ініціали)
Нормоконтроль	(підпис)	Тиш Є.В. (прізвище та ініціали))
Завідувач кафедри	(підпис)	Осухівська Г.М. (прізвище та ініціали)
Рецензент	(підпис)	Мацюк О.В. (прізвище та ініціали)

м. Тернопіль – 2021

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

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Осухіська Г.М.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

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

за спеціальністю 123 Комп'ютерна інженерія
студенту Шевчуку Юрію Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби автоматичного розпізнавання особи в домофонних системах

Керівник роботи *Стадник Наталія Богданівна, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «__28__» _жовтня_ 2021 року №__4/7-916_

2. Термін подання студентом роботи 22.12.2021

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1 Аналітична частина. 2 Теоретична частина. 3. Практична частина. 4 Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема, мета, задачі, об'єкт, предмет дослідження. 2. Актуальність дослідження. 3 Основні методи розпізнавання людини за біологічними ознаками. 4. Структура процесу розпізнавання за зображенням обличчя. 5. Основні методи підвищення точності алгоритмів розпізнавання зображення особи. 6. Виділення та попередня обробка зображення обличчя. 7. Загальна структура системи із застосуванням модуля розпізнавання відвідувача 8. Діаграма прецедентів. 9. Результати випробувань. 10. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., доцент	01.11.21	07.12.21
Безпека в НС	Стадник І. Я., професор	01.11.21	09.12.21

7. Дата видачі завдання _____ 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи	28.10.21	Виконано
2	Аналіз літературних джерел	29.10.21-18.11.21	Виконано
3	Обґрунтування актуальності дослідження	18.11-21.11.21	Виконано
4	Аналіз предмету дослідження та предметної області	21.11-26.11.21	Виконано
5	Проведення дослідження методів та засобів аналітичного опрацювання даних	22.11-30.11.21	Виконано
6	Оформлення розділу «Аналітична частина»	20.11-26.11.21	Виконано
7	Оформлення розділу «Теоретична частина»	27.11-02.12.21	Виконано
8	Оформлення розділу «Практична частина»	03.12-10.12.21	Виконано
9	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-12.12.21	Виконано
10	Нормоконтроль	11.12-14.12.21	
11	Попередній захист роботи	15.12.21	Виконано
12	Захист кваліфікаційної роботи	23.12.21	

Студент _____ *Шевчук Ю.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник Н.Б.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби автоматичного розпізнавання особи в домофонних системах // Кваліфікаційна робота за освітнім рівнем «магістр» // Шевчук Юрій Вікторович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІм–61 // Тернопіль, 2021 // с. – 69, рис. – 22, табл. – 6 , аркушів А1 – 10 , бібліогр. – 30.

Ключові слова: ДОМОФОННА СИСТЕМА, РОЗПІЗНАВАННЯ ОСІБ, БІОМЕТРІЯ, ВІДЕО, КОНТРОЛЬ ДОСТУПУ

Кваліфікаційна робота присвячена дослідженню способів автоматичного розпізнавання особи в домофонних системах. Проаналізувавши способи розпізнавання людини було визначено біометричну ознаку, за якою можна ідентифікувати особу в домофонних системах. Метод розпізнавання, котрий базується на геометрії обличчя, має найкраще співвідношення точності і зручності та може бути використаний як основний виконання поставленого завдання. Були досліджені існуючі методи локалізації обличчя на зображенні, нормалізації, класифікації та обрані оптимальні для ефективного вирішення поставленої задачі. Розпізнавання за зображенням особи при доступі в приміщення може бути як додатковий спосіб або комбінувати з існуючими.

В результаті був розроблений алгоритм ідентифікації відвідувачів за зображенням обличчя в домофонних системах, виконана його програмна реалізація. Розроблений програмний засіб, який реалізує запропонований алгоритм, можна застосовуватися при розробці модулів систем для контролю доступу в приміщення з невеликими базами зареєстрованих осіб (15-20 осіб). Це можуть бути приватні будинки, невеликі офіси, службові приміщення тощо.

ANNOTATION

Methods and tools for automatic recognition of visitors in intercom systems // Master thesis // Shevchuk Yuriy // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Systems and Nets, group CIm - 61 // Ternopil, 2021 // p. – 69, fig. – 22 , table. – 6, Sheets A1 - 10 , Ref. - 30.

Keywords: INTERCOM SYSTEM, PERSONS RECOGNITION, BIOMETRY, VIDEO, ACCESS CONTROL

The thesis deals with the study of methods of automatic face recognition in intercom systems. After analyzing the methods of human recognition, a biometric feature was identified, which can be used to identify a person in intercom systems. The recognition method, which is based on facial geometry, has the best ratio of accuracy and convenience and can be used as the main task. The existing methods of facial localization in the image, normalization, classification were studied and the optimal ones were selected for the effective solution of the set task. Face recognition when entering the room can be as an additional method or combined with existing ones.

As a result, an algorithm for identifying visitors by face image in intercom systems was developed, and its software implementation was performed. The developed software, which implements the proposed algorithm, can be used in the development of intercom systems to control access to premises with small databases of registered persons (15-20 people). These can be private homes, small offices, office space etc.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

AdaBoost (adaptive boosting) - адаптоване поліпшення, алгоритм машинного навчання

PCA (Principal Component Analysis) – МГК (метод головних компонент)

АП - абонентський пристрій

БД – база даних

Біометрія - це методи автоматичної ідентифікації людини і підтвердження особи людини, засновані на фізіологічних або поведінкових характеристиках

БО – біометричні ознаки

Бустінг – процедура послідовної побудови композиції алгоритмів машинного навчання, коли кожен наступний алгоритм прагне компенсувати недоліки композиції всіх попередніх алгоритмів

ДС - домофонна система

ІХПІ – ймовірність хибнопозитивної ідентифікації

ІЧ - інфрачервоне

ЛБШ – локальний бінарний шаблон

МРВ - модуль розпізнавання відвідувача

ХСО – характерні симетричні ознаки

ПЗ – програмне забезпечення

ПК - персональний комп'ютер

ПВ – панель виклику

РОО – райдужна оболонка ока

СКУД - система контролю і управління доступом

ЗМІСТ

ВСТУП

Актуальність теми. За останній час ДС перетерпіли ряд еволюційних змін, на ринок виходять більш досконалі рішення. Використання сучасних мережевих технологій дозволило перейти від координатно-матричних систем до систем, котрі базуються на протоколах TCP/IP. Розвиток ринку мікропроцесорів дозволив значно поліпшити апаратну частину. Розвиток мобільних технологій збільшив доступність систем, за рахунок можливості замінити абонентські трубки мобільними пристроями. Все це направлено на підвищення ефективності експлуатації подібного роду систем, і відкриває нові можливості для впровадження інших ще більш досконалих функцій.

Контроль доступу в приміщення за допомогою ДС, одна з ключових функцій системи, від ефективності якої залежить безпека мешканців, співробітників і збереження майна. На жаль пропоновані на ринку системи не можуть в достатньому обсязі забезпечити ефективний контроль осіб в приміщення. Перш за все це обумовлено недовершеністю механізмів доступу за допомогою електронних ключів або набором коду доступу. Використання для доступу такої ознаки відвідувача, яка притаманне тільки йому і не може бути використана іншими особами, значно б збільшило ефективність системи при вирішенні задачі контролю доступу. Такі технології існують і широко застосовуються в більш складних системах банківської сфери, криміналістики, в системах контролю і управління доступом на підприємствах, які засновані на ідентифікації особи людини за БО.

За останнє десятиліття, дослідження в області біометрії значно просунулися, з'явилася достатня кількість доступних методів, котрі дозволяють ідентифікувати особу людини за зображенням обличчя, відбитку пальців, поведінці та іншим ознакам. Враховуючи сказане вище, можна припустити, що розпізнавання користувача за БО цілком може бути реалізовано і в сучасних ДС.

Мета дослідження: за рахунок автоматичної ідентифікації особи відвідувача, підвищити ефективність контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС.

В роботі поставлено та розв'язано **наступні задачі**:

– дослідження існуючих способів ідентифікації особи за БО;

– формулювання критеріїв для порівняння існуючих систем;

– визначення і програмна реалізація найбільш ефективного алгоритму автоматичної ідентифікації особи відвідувача в ДС;

– розробка дослідного зразка, який би експериментально довів ефективність виявленого алгоритму.

Об'єкт дослідження: процес розпізнавання особи за БО.

Предмет дослідження: технології для розпізнавання особи за БО.

Методи дослідження: Метод теоретичного дослідження та експериментальний з використання персонального комп'ютера. Методологічну основу дослідження становлять фундаментальні положення комп'ютерної на програмної інженерії, наукові дослідження вітчизняних і зарубіжних компаній та вчених у сфері трасування кабельних мереж.

Наукова новизна отриманих результатів.

– обгрунтовано особливості методів підвищення точності алгоритмів розпізнавання зображення особи;

– запропонований ефективний алгоритм автоматичної ідентифікації особи відвідувача в ДС;

– розроблено вбудований програмний засіб для розпізнавання користувача за зображенням обличчя;

– на основі проведених тестувань розробки запропоновано збільшувати кількість шаблонів обличь для кожного зареєстрованого відвідувача для кращого розпізнання його особи.

Практичне значення одержаних результатів. Розроблений програмний засіб, який реалізує запропонований алгоритм, може застосовуватися при розробці модулів ДС для контролю доступу в приміщення з невеликими базами зареєстрованих осіб, близько 15-20 осіб. Це можуть бути приватні будинки, невеликі офіси, службові приміщення тощо. Проведення додаткових досліджень, спрямованих на виявлення більш досконалих методів компенсації зміни освітленості в отриманих зображеннях осіб, а так само методів класифікації дозволить підвищити надійність алгоритму і застосовувати програмні рішення на його основі в більш широкій сфері, де для контролю доступу використовуються ДС.

Публікації. Результати дослідження апробовано на IX науково-технічній конференції «Інформаційні моделі, системи та технології» у вигляді опублікованих тез:

Шевчук Ю.В. Алгоритм ідентифікації відвідувача в домофонній системі за зображенням особи. Інформаційні моделі, системи та технології: Праці IX наук.-техн. конф. (Тернопіль, 08-09 грудня 2021 р.), Тернопіль, 2021. – С. 143.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів, висновків, списку використаної літератури та додатків. Обсяг роботи: пояснювальна записка – 69 арк. формату А4, графічна частина – 10 аркушів формату А1.

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1. Етапи розвитку домофонії

Історія домофона почалася порівняно недавно. Свої витоки зародження пристрою по забезпеченню безпеки приміщень, бере в другій половині XX століття, коли населення країни задумалося про захист свого житла або офісу [1].

Перший етап становлення домофонів можна віднести до 1970-х років, коли владою було здійснено спробу захистити будинку від небажаних відвідувачів. В цей час на вхідних дверях з'явилися металеві коробки з кнопками (система «Мосліфт» [2]), за допомогою яких, при наборі визначеної комбінації цифр, мешканець будинку міг не тільки потрапити в будинок, але і зв'язатися з диспетчером комунальної служби району.

Другий етап відноситься до кінця 1980-х початок 1990-х рр. Новий клас обладнання - це переговорний і замковий пристрій одночасно. Головною відмінною рисою нового домофона від попередника стала можливість жителям будинків вільно проходити в під'їзд за допомогою спеціального ключа, що виключало витік інформації про код доступу. Новинкою став і сам переговорний пристрій, за допомогою якого людина, перебуваючи в будинку, могла за голосом дізнатися про того, хто прийшов і вирішити, відкривати двері чи ні, не виходячи з квартири. В цілому, другий етап становлення домофонів показав досить високу ефективність щодо захисту під'їздів від непрошених гостей, а також дозволив підготувати основну масу мешканців до так званої «домофонізації» житлового сектора і поступово перевести цей пристрій з розряду елітного в розряд масового.

Третій етап починається з кінця 1990-х рр. Головною його особливістю є прийняття ряду документів на урядовому рівні, де була зазначена проблема і поставлені організаційно-правові питання по встановленню домофонів та кодових замків в житловому секторі будинків. Основний акцент робився на використанні

технічних засобів охорони, в тому числі СКУД, до яких можна віднести і домофони. Прогрес не стояв на місці і в цей час були створені кілька вдалих моделей домофонів, серед яких був і відеодомофон. Особливістю відеодомофона стала передача не тільки звуку, але і зображення гостя, котрий прийшов.

До четвертого етапу можна віднести останнє десятиліття. На ринку стали з'являтися ДС, із застосуванням IP технологій. Використання стека протокола TCP/IP для зв'язку між компонентами системи дозволило спростити її монтаж, передача в цифровому вигляді аудіо та відео інформації підвищити ефективність комунікації між абонентами і відвідувачами. Компоненти системи стали реалізовуватися на більш досконалій елементній базі, що дозволило використовувати спеціалізоване ПЗ для підвищення функціональності пристроїв.

1.2. Контроль доступу в ДС

Введення персонального коду доступу. Даний спосіб був реалізований ще в найперших моделях домофонів. Для доступу в приміщення відвідувач повинен набрати код доступу на клавіатурній панелі. Попередньо код доступу вноситься в пам'ять домофона, при налаштуванні системи адміністратором. При необхідності доступ за обраним кодом може бути закритий повністю або в визначені проміжки часу. Недолік даного способу, в тому, що будь-який код згодом ставав відомим стороннім особам, що істотно позначається на ефективності контролю доступу. У деяких сучасних системах дана функція може бути відключена.

Доступ за допомогою контактних і безконтактних ключів. Зараз є найбільш поширеним способом. Доступ в приміщення здійснюється за допомогою електронних ключів, контактних Touch Memory [4] і без контактних RFID [5]. Такий електронний ключ підноситься до зчитувального пристрою і у випадку ідентифікації ключа останнім, подається сигнал на відмикаючий пристрій. Невеликий розмір контактного ключа дозволяє прикріплювати його практично на будь-якому носії - виробі, брелоку. Як RFID-мітки можуть застосовуватися різні

пластикові брелоки, карти мають вбудований чіп, які передають свій індивідуальний виділений номер при піднесенні ключа в полі дії зчитувача домофону. Зазвичай ця відстань не перевищує 10 см. Живлення ключа (брелока або карти) відбувається від енергії, котра випромінюється антеною зчитувача.

Основний недолік для контактних ключів - це слабкий вандалозахист самого зчитувача: вплив електрошокером, п'єзозапальнички або стрибок напруги в мережі можуть вивести прилад із ладу. RFID - в цьому плані більш надійні, але так само як і Touch Memory не можуть гарантувати ззахист від проникнення в приміщення сторонніх осіб. З причини поширення технології, деякі спеціалізовані фірми пропонують універсальний ключ, який дозволить відкрити до 80% приміщень, в яких для контролю доступу використовується та чи інша ДС. Також хоч і до незначного, але все таки недоліка, можна віднести і те, що ключ можна втратити або зламати, а придбання нового ключа коштує грошей.

Біометрична ідентифікація. Останнім часом одержали широкий розвиток системи, засновані на біометрії. Вони застосовуються в криміналістиці, медицині, в банках, в системах контролю доступу та в інших галузях. Осторонь не залишилися і виробники ДС. Домофони з функцією біометрії дозволяють ідентифікувати відвідувача за його фізіологічним ознаками, і в разі успіху надати доступ в приміщення. Такі системи не вимагають наявності ключа для отримання доступу, в цьому випадку сама фізіологічна ознака відвідувача така як обличчя, голос, відбиток пальця є ключем доступу. Підробити таку ознаку достатньо складно, а в деяких випадках навіть неможливо, що може вирішити проблему доступу незареєстрованих осіб в приміщення. В цілому технологія перспективна, але з причини своєї новизни, системи на її основі достатньо коштовні і працюють при обмежених зовнішніх умовах. В даний час методи розпізнавання за БО постійно удосконалюються, роблячи цю технологію більш надійною, і як наслідок, рішення на її основі можуть бути більш ефективними у порівнянні з іншими способами контролю доступу.

1.3. Аналіз і порівняння методів розпізнавання людини за БО

1.3.1. За відбитком пальця

Внутрішня поверхня долоні і ступні людини містить дрібні боріздки, які утворюють малюнок, котрий мало залежить від генів. Дана властивість дозволяє використовувати відбитки пальців для ідентифікації людини. Існуючі алгоритми розпізнавання за відбитками пальців використовують множину деталей папілярних візерунків. Наприклад, найбільш часто використовується роздвоєння і кінець борозенки, звані деталями, які добуваються з оцифрованого відбитка. Процес добування властивостей відбитка зазвичай починається з оцінки якості зображення. Кожен опублікований метод добування властивостей починається з обчислення орієнтації борозенок, яка відображає точний напрямок борозенок на кожному пікселі. Ця орієнтація борозенок використовується для налаштування фільтра параметрів, щоб поліпшити якість зображення і сегментації борозенок. З сегментованих борозенок для локалізації деталей обчислюється розріджене зображення. Зазвичай після цього відбувається очищення зображення від деяких помилкових рис, що з'явилися внаслідок недосконалості відбитка пальця (бруд, порізи). Специфіка папілярного малюнка стає неповторним кодом, котрий зберігає повну інформативність самого відбитка. Власне саме «коди відбитків пальців» і є збереженими в БД, котру застосовують для пошуку і порівняння [7].

Спочатку для зняття відбитків використовувалися чорнило і чистий аркуш паперу, досить було притиснути палець, попередньо покритий чорнилом, до аркуша паперу і можна було отримати його відбиток. На даний момент розроблено багато різних технік зняття відбитків без допомоги чорнила. Основний принцип таких методів - розпізнавання борозенок на пальцях, які прикладають до поверхні сканера. Сканери можуть бути реалізовані за різними технологіям, серед них варто згадати: повне внутрішнє відображення і інші оптичні методи; ємнісний опір; термічні сенсори; ультразвукові сенсори.

На даний момент цей тип розпізнавання, мабуть, найпоширеніший спосіб розпізнавання людини за БО. Широко використовується в СКУД, в мобільних телефонах, в криміналістиці.

1.3.2. За геометрією обличчя

В основі усіх існуючих методів розпізнавання за обличчям лежить той факт, що обриси лиця і форма черепа є індивідуальні для окремої особи. На даний момент визначено два напрямки, за якими ведуться дослідження методів розпізнавання за обличчям. Це різні методи, в основі яких лежить двовимірне і тривимірне зображення обличчя [8]. Методи, котрі базуються на двовимірному зображенні обличчя, розроблені достатньо давно. Основною сферою їх застосування була і є криміналістика, що і сприяло їх бурхливому розвитку. Вподальшому з'явилося комп'ютерне представлення методів, що зробило його надійнішим. В даний час через недостатню надійність статистичних показників цей спосіб розпізнавання застосовується в мультимодальній біометрії.

Основна перевага методів при двовимірному розпізнаванні, в тому, що не має потреби у дороговартісному устаткуванні. При наявності відповідного обладнання можна забезпечити розпізнавання на достатньо великих від камери відстанях. Варто навести і недоліки такого методу, основний - залежність статистичних показників від освітленості, зокрема, не має змоги фіксувати обличчя людей у сонячний день, котрі заходять з вулиці у приміщення. Наявність будь-яких додаткових зовнішніх атрибутів, як то окуляри, борода і т.п. для багатьох алгоритмів є неприйнятними. Обов’язковим є фронтальне зображення обличчя, з дуже незначними відхиленнями. Необхідно відмітити, що значна кількість алгоритмів не враховують ймовірні зміни міміки обличчя, іншими словами вимагається постійна нейтральність виразу лиця.

Програмна реалізація методів, заснованих на тривимірному розпізнавання, є достатньо складною задачею. Найбільш відомим класичним методом вважається

метод проектування шаблону. На обличчя проектується сітка, потім камера виконує фото зі швидкістю десятки кадрів за одну секунду, і одержані зображення треба опрацювати спеціальним ПЗ. Проекція променя, котрий падає на поверхню достатньої кривизни, згинається, чим більше поверхня викривлена, тим більший власне і вигин такого променя. Потім маючи отримані знімки треба відновити 3D модель обличчя, на якій потрібно визначити та видалити перешкоди (вуси, бороду, окуляри і т.п.). Вподальшому треба проаналізувати модель – виділити особливості антропометрії, котрі в результаті і будуть записані в унікальний код при поміщенні в БД. Також стає популярним метод розпізнавання за зображенням, яке одержано з використанням кількох камер.

Метод має наступні переваги: є низько чутливим до вияву зовнішніх факторів (чи на людині, чи на її оточенні); висока надійність (на рівні з ідентифікацією за відбитками пальців). Варто вказати і на недоліки: будь-які зміни у міміці лиця чи наявність якихось перешкод на ньому негативно впливають на статистичну надійність цього методу. Для зменшення ймовірності підробки зображення обличчя, необхідно застосовувати більш складні алгоритми розпізнавання і конструкції зчитувальних пристроїв (стереопара), що може вплинути на вартість.

1.3.3. За РОО

РОО є унікальним атрибутом кожної людини. Її візерунок починає формуватися на восьмому місяці внутрішньоутробного розвитку, досягає остаточної стабілізації, коли людина має біля двох років і фактично є незмінним упродовж усього її життя. На зміну візерунка можуть вплинути або сильні травми ока або різкі патології. Серед усіх наявних біометричних методів цей метод вважається одним з найточніших [8].

За будовою система ідентифікації особи за РОО поділяється на дві частини. Перша, це пристрій захоплення зображення, первинного опрацювання і передачі

обчислювачеві. Друга, власне, обчислювач, котрий проводить порівняння наявного зображення із тим, яке присутнє в БД. Саме обчислювач і здійснює передачу вказівки про допуск виконавчому пристрою. Тривалість первинного опрацювання зображення в існуючих системах орієнтовно становить 300-500 мс, швидкість проведення порівняння одержаного зображення з БД порядка 50 -150 тисяч порівнянь за одну секунду. При застосуванні ж спеціалізованих обчислювачів та алгоритмів оптимізації пошуку можна навіть ідентифікувати конкретну людину серед усіх жителів визначеної країни.

Метод володіє рядом переваг, зокрема статистична надійність його алгоритму роботи. Фіксацію зображення РОО можна проводити на відстані від кількох сантиметрів навіть аж до кількох метрів, необхідно відмітити, що людина фізично не контактує з пристроєм. РОО володіє захистом від пошкоджень, а, отже, часово не змінюватиметься. Також можливе застосування значного різноманіття методів, котрі вберігають від підробки. Разом з тим метод має і недоліки – вартість такої системи, котра базується на РОО більша, ніж вартість системи, в основі якої лежить розпізнавання пальця або обличчя. Також варто згадати і низьку доступність готових технічних рішень.

1.3.4. За венами руки

Є новим словом в сфері біометрії, широке її використання почалося лише упродовж останніх 15 років. ІЧ-камера проводить фотографування зовнішньої або внутрішньої частини руки. Венозний візерунок створюється через те, що гемоглобін поглинає ІЧ- випромінювання. Як наслідок ступінь відображення стає меншим, таким чином вени на камері вени відображаються чорними лініями. ПЗ на основі одержаної інформації формує цифрову згортку. Необхідно зауважити, що контакту «живого» людини зі сканером не вимагається. Технологію можна порівняти за надійністю із розпізнаванням з РОО [8].

Метод володіє рядом переваг: не має потреби у безпосередньому контакті зі сканером. Висока достовірність, отримані статистичні показники методу порівнюються із показниками РОО. Додатковою перевагою є прихованість атрибуту, тобто складно одержати цей атрибути від людини «на вулиці», наприклад, зазнімкувавши її. Поряд з перевагами метод має і недоліки – неприпустимим є засвічення скануючого пристрою променями сонця та ламп. Також окремі вікові захворювання, як то артрит, статистичні характеристики роблять значно гіршими. Метод менше розвинений порівнюючи з іншими відомими статичними методами біометрії.

1.3.5. За сітківкою ока

Цей метод взяв кращі риси методів ідентифікації за РОО і за венами руки людини. Капілярний візерунок на поверхні сітківки ока фіксується сканером. Сітківка володіє нерухомою структурою, котра є незмінною в часі. На структуру сітківки вплинути може хіба результат хвороби [8]. Технічно процес сканування сітківки проходить із застосуванням ІЧ- та низької інтенсивності світла, котре спрямовується через зіницю до кровоносних судин на задній стінці ока. Такі сканери широкого використовуються в СКУД на секретних об'єктах, оскільки вони мають надзвичайно малий відсоток відмови зареєстрованим користувачам в доступі і при їх використанні помилковий доступ практично виключений.

Метод володіє рядом переваг: висока статистична надійність; завдяки малій поширеності систем мала можливість розробки способу їх «обману». Разом з тим недоліками методу є: складність при застосуванні (оскільки система має великий час опрацювання); дороговартісна система; немає великого ринку пропозицій, тому, як наслідок, метод слабко розвивається. Психологічний фактор, користувачі відчувають дискомфорт при скануванні сітківки, деякі намагаються уникнути подібного методу ідентифікації боячись пошкодити свої очі.

1.3.6. За геометрією руки

У цьому методі використовують два основних підходи. Перший базується виключно на геометрії кисті, тоді як другий - на змішаних геометричних та образних параметрах. Власне до них належать образи на згинах між фалангами пальців, візерунків підшкірних кровоносних судин [7].

Суть першого підходу полягає в тому, що вся інформація, котра цікавить, сформована в горизонтальному і вертикальному обрисі людської кисті. Основні БО руки: ширина долоні, радіус вписаного в неї кола, довжина і ширина пальців, висота кисті в трьох визначених пунктах. Ряд інших алгоритмів може використовувати до 21-єї геометричних ознак руки. Відмінною рисою даного методу є його простота. Окрім цього кожен еталон людської руки можна представити надзвичайно стисло у вигляді вектора значень атрибутів.

Суть другого підходу - «зняття» з руки чотирьох атрибутів, з яких три є скалярними величинами і відносяться до розмірів пальців, тоді як четвертий є півтонуванням складок шкіри на згині між фалангами. Власне три перші атрибути - це ширина і висота вказівного пальця, а також довжина середнього пальця. Останній атрибут є зображенням складок шкіри на згині між середньою і нижньою фалангами вказівного пальця. Існування біометричного параметру руки у вигляді напівтонового зображення істотно ускладнює, на відміну від першого підходу, виготовлення муляжу, який може бути застосований для взлому системи ідентифікації. Як четверта характеристика може бути обрана будь-яка інша або кілька. При цьому варто зазначити, що виробник, який постачає на ринок системи такого виду, не надає точних даних про ознаки руки, котрі використовуються в системах. Цей факт також ускладнює створення муляжу руки.

Переваги методу - нескладна процедура одержання образу, не ставляться високі вимоги до зображення. Крім того, розмір одержаного шаблону буквально кілька байт. Температура, вологість або забруднення не мають впливу на аутентифікацію особи. Підрахунки, котрі треба виконати для порівняння з

еталоном, є дуже простими. Недоліки методу - на точність ідентифікації системи може впливати спотворення структури руки, викликане розпухання тканин, забоями. Артрит, наприклад, може сильно перешкодити використанню сканера.

1.3.7. За голосом

Користувач, якого попередньо зареєстровано в системі, говорить персональний ідентифікатор, котрий є реєстраційним номером. Також він може промовити парольне слово або фразу. При текстозалежному розпізнаванні пароль є відомим для системи верифікації та вона «вимагає» від користувача промовити його. Пароль з’являється на екрані, і людина повинна промовити його у мікрофон. При текстонезалежному розпізнаванні парольне слово користувача не збігається з еталонним. Звідси, як пароль користувач може говорити будь-яке слово або фразу. Після цього система приймає вимовлений сигнал, певним чином опрацьовує його і вирішує, або прийняти або відмовити у прийнятті запропонований ідентифікатор користувача. Система верифікації здатна попередити користувача про недостатній збіг його голосу з наявним в БД еталоном і попросити промовити додатковий текст для прийняття фінального рішення [9].

Переваги методу - не вимагає дорогої апаратури, сканером може бутим звичайний мікрофон. Ненав'язливий, розпізнавання відбувається на відстані, не затримуючи і не відволікаючи людину. Недоліки методу - голос формується з комбінації фізіологічних і поведінкових факторів, тому у даного методу найбільш низька точність ідентифікації в порівнянні з представленими вище методами. Зокрема у людини із застудою можуть бути труднощі з використанням таких систем. Щоб обдурити систему достатньо просто відтворити запис з магнітофона.

1.4 Порівняльний аналіз аналогів

Як було сказано вище, в даний час виробники ДС реалізують рішення, в яких використовують біометрію для контролю доступу. Здебільшого на ринку переважають системи, в яких для ідентифікації використовуються такі БО як відбитки пальців і зображення обличчя, або комбінація цих методів з введенням коду доступу - верифікація.

Система «Gira door communication system». Це рішення від німецького виробника, компанії GIRA, для організації ДС за модульним принципом в приватному або малоквартирному сегменті [10]. Функція розпізнавання користувача реалізується за допомогою модуля Fingerprint [11], який здійснює контроль доступу на підставі біометричних особливостей людського пальця. Використовуючи технології високочастотного сканування, він сканує структури глибокого шару шкіри того пальця, який людина прикладає до приладу. Стан пальця відвідувача постійно перевіряється пристроєм, кожного разу, за необхідності, розраховується його образ. Це особливо важливо для дитячих пальців, оскільки вони з часом змінюються, і така процедура вносить в запам’ятований образ необхідні зміни. Біометричним модулем може оброблятися до 50 різних відбитків пальців. Налаштування здійснюється без будь-якого комп'ютера або ПЗ. На кожен відбиток пальця можна запрограмувати окрему функцію - відкриття дверей, виклик абонента, включення / виключення зовнішнього джерела освітлення.

До недоліків даного рішення можна віднести втрату можливості надбудов модуля Fingerprint в разі втрати пальця адміністратора або якщо та людина, котра раніше виконувала функції адміністратора більше такими питаннями не займається. Також варто відзначити, що для зміни налаштувань доступу необхідна присутність того користувача відбиток пальця, якого потрібно видалити зі списку доступних. Найістотнішим недоліком є ціна самої системи.

Нижній температурний межа модуля Fingerprint обмежений -20 С, що робить обмеженою експлуатацію в регіонах з різко континентальним кліматом.

Біометричний зчитувач ST-FR040EM марки Smartec. Призначений для використання в системах контролю доступу та обліку робочого часу в якості пристрою розпізнавання користувача за геометрією обличчя. Також може використовуватися в автономному режимі для безпосереднього управління електрозамком вхідних дверей. На передній панелі пристрою розташовані дві камери, звичайна і така, яка працює в ІЧ-діапазоні. Зображення осіб, отримані з кадрів, знятих ІЧ-камерою використовуються для розпізнавання. Камери розташовані під кутом до вертикальної площини, що дозволяє забезпечити найбільш вигідний ракурс для зйомки обличчя.

Пристрій підтримує два режими розпізнавання за обличчям, верифікація (1 : 1) і ідентифікація (1 : N). В режимі верифікації, зображення обличчя, котре отримане ІЧ-камерою, порівнюється з шаблоном обличчя, який зберігається для вказаного ПІН-коду. При ідентифікації, пристрій порівнює зображення обличчя з усіма шаблонами, що зберігаються в пристрої. За відповідності, відправляється сигнал на контролер відкриття дверей і робиться запис у журнал подій, із збереженням даних користувача. Шаблони обличчя в сховищі пристрою додаються за допомогою зйомки ІЧ-камерою користувача, з послідовною зміною ракурсу зйомки особи. Зчитувач може програмуватися як автономно, так і за допомогою спеціалізованого ПЗ, встановленого на комп'ютері та підключеного до тієї ж мережі, що і зчитувач. Перевагою даного пристрою є ціна, вона нижче ніж у попереднього аналога. Недоліки - не може бути використана в ДС. Має робочий діапазон температур, прийнятний тільки для експлуатації в приміщеннях.

Домофон з біозчитувачем компанії FERMAX. Рішення від іспанського виробника FERMAX [12]. Компанія пропонує домофони зі зчитувачами відбитків пальців як вбудовані в ПВ, так і у вигляді окремих модулів, які можуть використовуватися як автономний пристрій. Автономні модулі зчитування відбитків пальців можуть бути використані в системах де не потрібно мати

складний контроль доступу без реєстрації подій. В цілому набір функцій і принцип роботи аналогічний до подібних систем, наприклад, згаданому в п. 1.4.1.

Для порівняння існуючих аналогів запропоновані критерії, зазначені в таблиці 1.1. Як видно з таблиці існуючі системи мають ряд недоліків, зокрема це їх вартість і температурні умови.

Таблиця 1.1

Критерії порівняння аналогів

Критерій	Gira	ST-FR040EM	FERMAX
Вартість	від 4 000 $ USA	400 $ USA	9000 €
Температурні умови	від -20 °C до +70 °C	від 0 °C до +50 °C	від -10 °C до +55 °C
Ємність бази еталонів	50 відбитків пальців	500 шаблонів обличь	3000 відбитків пальців
Час розпізнавання	< 1,5 с	< 2 с	< 1 с

1.5. Висновки до розділу

В цьому розділі наведені етапи розвитку домофонії. Описано особливості контролю доступу в ДС. Набір коду доступу на ПВ, використання контактних або безконтактних ключів, в даний час є найбільш поширеним способом отримання доступу в приміщення. Проаналізовано різні методи розпізнавання людини за БО. Кожен із проаналізованих методів має свої переваги і недоліки. Метод розпізнавання, котрий базується на геометрії обличчя, має найкраще співвідношення точності і зручності та може бути використаний як основний для автоматичного розпізнавання користувача в ДС. Здійснено порівняння існуючих на ринку аналогів ДС.

РОЗДІЛ 2
ТЕОРЕТИЧНА ЧАСТИНА

2.1. Аналіз методів розпізнавання за зображенням обличчя

Зараз є велика кількість різних методів розпізнавання людини за зображенням лиця, котре одержане за допомогою відео або фотокамери. Завдання, для вирішення яких застосовуються ті чи інші методи, досить різні, наприклад, розпізнавання особи в потоці, чи за поганих умов освітленості, або за наявності перешкод (борода, вуса, окуляри), або за різних ракурсів і т.п.

Для вирішення певної задачі обраний метод може бути достатньою точно ефективним, тоді як в іншому випадку, навпаки, за рахунок своєї статистичної ненадійності малозастосовним. Таким чином, для виявлення переліку найбільш ефективних методів вирішення поставленого завдання має сенс проаналізувати зображення обличчя відвідувача, отриманого з відеокамери ПВ. Розглянемо випадок, при якому відвідувач потрапляє в кадр відеокамери домофона. Перш ніж отримати доступ в приміщення, відвідувач натискає кнопку виклику абонента на ПВ або номер його квартири. Чекаючи відповіді від абонента погляд відвідувача переважно направляється в сторону ПВ, що дозволяє відобразити його обличчя відеокамерою в найкращому ракурсі для розпізнавання - анфас. Якщо приміщення має кілька входів, на кожному з яких встановлена ПВ, при зйомці відвідувача фон на різних кадрах може відрізнятися і бути неоднорідним. При зміні часу доби змінюється і освітленість в кадрі, особливо характерно для ПВ, встановлених на вулиці. За занадто поганої освітленості включається ІЧ підсвічування, через яке, кадри, котрі знімаються відеокамерою, стають чорно-білими.

Крім іншого необхідно враховувати і той факт, що для захоплення максимальної дверного простору в кадрі, деякі виробники роблять об'єктив відеокамери ширококутним, що може позначитися на пропорціях особи в одержуваних зображеннях.

Таблиця 2.1

Характеристики зображення відвідувача, отримані в момент виклику

Характеристика	Значення
Середній розмір зображення обличчя в кадрі	приблизно 144 x 148 пкс (10%)
Кольоровість	чорно-біла / кольорова
Оточуючий фон	неоднорідний
Ракурс зйомки	анфас
Попадання обличчя в кадр	повне
Вираз обличчя	нейтральне
Відстань між об'єктом спостереження і камерою	приблизно 300 – 500 мм

2.2. Задачі розпізнавання осіб на зображеннях і методи їх вирішення

Попри значну кількість існуючих методів, можна визначити загальну структуру, притаманну процесу розпізнавання осіб (див. рис. 2.1)

Рис. 2.1. Структура процесу розпізнавання за зображенням обличчя

Зі структури процесу, зображеної на рис. 2.1 видно, що для вирішення головного завдання розпізнавання осіб, необхідно вирішити завдання більш низького рівня такі як, детектування особи на зображенні, нормалізація локалізованої особи, обчислення ключових ознак і порівняння їх з еталоном.

Для вирішення кожної підзадачі існує певний набір методів, від ефективності яких залежить завдання розпізнавання в цілому.

2.2.1. Детектування особи на зображенні

Перш за все необхідне визначити область зображення, яке містить обличчя. Існуючі методи вирішення цього завдання можна розбити на чотири категорії [14]: емпіричний; ХСО; заснований на шаблонах, заданих розробником; виявлення за зовнішніми ознаками.

Емпіричний метод. Заснований на алгоритмі, котрий реалізує норми, за якими визначається чи є фрагмент зображення людським обличчям чи ні. Ці норми – потреба у формалізації емпіричних знань як саме виглядає лице на зображеннях. Наприклад, одне з таких правила це те що обличчя містить двоє симетрично розташованих очей, рот, ніс, котрі значно відрізняються яскравістю від інших частин. Даний метод використовувався при перших спробах локалізувати особу на зображенні. Застосовувався на початкових етапах розвитку комп'ютерного зору за рахунок низьких вимог до обчислювальних ресурсів. Деякі методи мають цілком достойні показники по виявлення особи на однорідному фоні. Але метод не застосовують при локалізації особи на зображеннях, що містять велику кількість осіб і складний фон, що є його основним недоліком. Є чуттєвим до нахилу і повороту голови.

Метод ХСО. Заснований на виявленні закономірностей і властивостей зображення обличчя неявно, пошук інваріантних особливостей обличчя, без залежності від положення і кута нахилу. Процес складається з наступних етапів: детектування на зображенні очей, носа, рота; виявлення кордонів особи; поєднання знайдених інваріантних ознак і їх верифікація. Одним з переваг методу в порівнянні з попереднім, це можливість розпізнати обличчя в різних положеннях. Але ймовірність достовірного розпізнавання обличчя істотно падає

при загромадженні обличчя іншими об'єктами, засвічуванні зображення, виникненні шумів або наявність складного заднього фону.

Метод заснований на шаблонах, заданих розробником. Шляхом опису властивостей окремих областей особи і їх взаємного розміщення формується якийсь шаблон, перевірка областей зображення на відповідність йому дозволяє виявити обличчя на зображенні. Плюси методу полягають у відносно простій реалізації і непогані результати при наявності на зображенні нескладного заднього фону. З мінусів - трудомісткість обчислення шаблонів для різного положення обличчя і необхідність калібрування шаблону поблизу із зображенням обличчя.

Метод виявлення за зовнішніми ознаками. Частині зображення зіставляється певним чином обрахований вектор ознак, котрий застосовується для систематизації зображення на два типи - обличчя і не обличчя. Відшукання обличчя на зображеннях за допомогою даного методу визначається, як повний перебір всіх фрагментів прямокутної форми різного розміру зображення і перевірці кожного такого фрагмента на відмінність обличчя. З метою скорочення часу на виявлення обличчя даними способом використовуються різні методи скорочення ряду розглянутих частин. Найбільш важливе завдання – чітко визначити сильні класифікатори. Саме вони матимуть найвищий пріоритет для перевірки знайдених ознак в зображенні. Набір слабших класифікаторів необхідно зменшувати за рахунок схожості один на одного, а також видаленні класифікаторів, що виникли при шумових викидах. Категорія методів, заснованих на виявленні за зовнішніми ознаками, як показали дослідження, найбільш ефективна на сьогоднішній день. Важливо при використанні даного методу вирішити задачу виділення сильних і зменшення слабких класифікаторів. Існує безліч різних методик, але найкраще зарекомендували себе адаптивне поліпшення і заснований на ньому метод Віоли-Джонса [15,16]. Цей метод на даний момент найперспективніший для детектування обличчя за рахунок високої

продуктивності, низької частоти фальшивих спрацьовувань і великим відсотком істинних виявлень. Головними принципами методу є:

– береться інтегральне представлення зображення, котре дає змогу швидко обрахувати необхідні об'єкти;

– застосовуються ознаки Хаара, за рахунок яких і проходить пошук необхідного об'єкта;

– застосовується бустінг для вибору тих ознак для шуканого об'єкта, котрі найбільше підходять на визначеному фрагменті зображення;

– усі ознаки поступають на вхід класифікатора, котрий дає результат «істина» або «фальш»;

– застосовуються каскади ознак для швидкого відкидання саме тих вікон, в яких обличчя не було ідентифіковане.

Найкращий кут нахилу для роботи близько 30 °, саме тоді механізм добре працює і чітко розпізнає риси обличчя. Якщо ж кут нахилу більший, тоді відсоток виявлення працює з зображеннями в градаціях сірого. Існують модифікації методу які дозволяють підвищити рівень виявлення при великих кутах нахилу.

2.2.2. Нормалізація зображення обличчя

Результатом рішення задачі визначення особи, буде прямокутна область на зображенні, яка містить обличчя - кадр. Точність алгоритмів розпізнавання за обличчям залежить від наявності на такому кадрі зовнішніх факторів, які не належать до особи людини. На наявність таких факторів в локалізованому зображенні впливає ракурс зйомки і освітленість. Таким чином, перш ніж передати таке зображення обличчя для обчислення ключових ознак, необхідно його нормалізувати, щоб зображення детектованого обличчя і зображення еталонних обличь мали однаковий масштаб, яскравість, контрастність.

Зараз є велика кількість методів, котрі дозволяють виконати геометричне вирівнювання обличчя в кадрі. Наприклад, один з таких методів має на увазі

виділення центрів очей і перетворення зображення так, щоб центри очей розташовувалися на одній лінії з фіксованим відстанню між собою.

Варто відмітити, що фактично головною проблемою для методів розпізнавання за зображенням особи є зміна характеристик освітлення, погані умови освітлення або недостатність освітлення, що вимагає крім геометричного вирівнювання використовувати і яскравісне. Для зменшення впливу яскравості існує безліч алгоритмів обробки зображення, такі як лінійна і нелінійна корекція гістограм, гамма-корекція, логарифмічна корекція, «сірий світ», Гаусівський або медіанний фільтр для придушення шумів.

2.2.3. Обчислення ключових ознак і зіставлення з еталоном

Після вирішення попередніх завдань можна припустити, що всі зображення осіб, котрі необхідно розпізнати знаходяться в деякому стандартному вигляді. Рішення завдання розпізнавання зводиться до обчислення ключових ознак для зображень зразка і еталона, і порівняння за обраною метрикою їх векторів між собою. Залежно від того наскільки їх різниця перевищує заданий поріг можна вирішити відрізняється зображення зразка від еталону або ні. Також можна навчити якийсь алгоритм класифікації, котрий дозволить визначити схожість зображень, попередньо подавши на його вхід вектора ознак цих зображень.

На даний момент існує безліч методів, котрі здатні вирішити цю задачу. Далі представлені найбільш поширені.

Метод Eigenfaces. Є найпершою роботою по розпізнаванню за зображенням особи, був запропонований в 1991 р авторами MatthewTurk і AlexPentland [17]. В основі алгоритму лежить PCA, метою якого є зменшення розмірності простору ознак навчальної вибірки так, щоб вона максимально, але якомога краще описувала типові образи, котрі належать множині осіб. Ефективність методу падає, якщо на зображенні особи наявні суттєві зміни в освітленості чи виразі лиця. При дотриманні ідеальних умов точність розпізнавання може досягати 90%

Метод Fisherfaces. Даний алгоритм нечутливий до великих змін в освітленості і виразу обличчя в кадрі [18].

Метод гнучкого порівняння на графах. В даному методі особа представляється у вигляді графа вершини, якого розташовуються на ключових точках особи (губи, ніс, очі і т.п.). У кожній точці, котра відповідає вершині графа, обчислюються її характеристики - колір, інтенсивність, відгуки текстурних фільтрів Габора [19]. Метод має високу обчислювальну складність, низьку технологічність при запам'ятовуванні еталонів і залежить від розміру бази еталонних осіб. Його точність ненабагато краща, ніж в методів, наведених вище.

Метод заснований на ЛБШ. ЛБШ - простий оператор який вперше був описаний в 1996 р. [21]. Застосовується в комп'ютерному зорі для класифікації текстур. За допомогою ЛБШ можна описати окіл пікселя на зображенні в двійковому коді. За поріг береться значення інтенсивності центрального пікселя. Якщо значення інтенсивності пікселя околу перевищує поріг, то приймається значення «1» в іншому випадку «0». Таким чином виходить восьми-розрядний код, який описує окіл пікселя. Подальші дослідження оператора проводилися в напрямку зміни форми околу, замість квадрата брали коло, еліпс.

За допомогою кодів ЛБШ можна розрахувати дескриптор зображення особи. Для цього, зображення розбивається на області, для кожного пікселя області розраховується код ЛБШ, будується гістограма, яка відображає частоту появи пікселя з певним кодом в даній області. Потім отримані гістограми об'єднуються в одну загальну, яка і є дескриптором особи. Порівняти два вектора ознак можна різними способами, це порівнювання заякої-небудь метрикою, наприклад, косинусною метрикою, або навчивши метрики [21].

Метод інваріантний до лінійної зміни освітленості та менш вимогливий до обчислювальних ресурсів, тому достатньо добре зарекомендував себе в розпізнаванні осіб, в порівнянні з вищеописаними.

2.3. Методи підвищення точності алгоритмів розпізнавання зображення особи

На точність результатів систем розпізнавання за зображенням особи впливає ряд факторів, серед яких - неконтрольовані умови освітленості навколишнього середовища. Зображення, зняті при таких умовах, мають нерівномірний розподіл рівня сірого, що є причиною різної контрастності одержуваного зображення. Недостатнє освітлення і недосконаліть обладнання - причина появи шумів. Все це необхідно враховувати при розробці алгоритмів розпізнання.

Вирівнювання гістограми. Метод заснований на перетворення шкали яскравості таким чином, щоб всі рівні яскравості мали однакову частоту, а сама гістограма відповідала рівномірному закону розподілу (рис. 2.2).

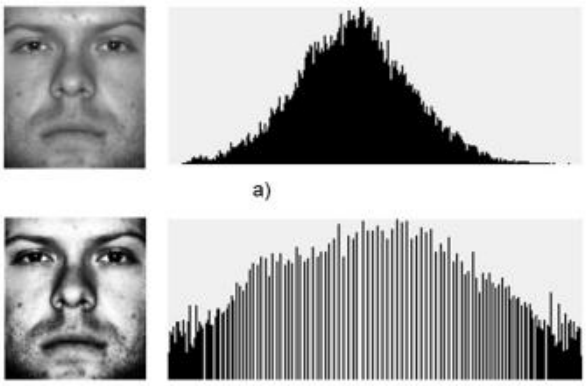

Рис. 2.2. Зображення обличчя до (а) і після (б) вирівнювання гістограми

В результаті такого перетворення у вихідному зображенні максимально використовуються всі можливі значення інтенсивності рівня яскравості, з приблизно однаковою кількістю пікселів для кожного значення. Відмінною рисою методу є те, що він може виконуватися повністю в автоматичному режимі, не вимагає додаткового налаштування параметрів, як це робиться, наприклад, в методах фільтрації. У деяких випадках, наприклад, коли частина зображення

обличчя закриває тінь, або різниця в освітленні правого або лівого боку значна, то застосування глобального вирівнювання гістограми може погіршити результат, в такому випадку застосовується локальне вирівнювання [22].

Гамма корекція. Не завжди лінійне перетворення яскравості зображення може покращити якість. Метод Гамма-корекції (див. рис. 2.3) заснований на нелінійній компенсації недостатньої контрастності зображення за рахунок степеневої функції $I_{вих} = K \cdot I_{вх}^{\gamma}$, де K - коефіцієнт; $I_{вих}$- значення інтенсивності вихідного зображення; $I_{вх}$ - значення інтенсивності вхідного зображення.

Рис. 2.3. Результат застосування Гамма корекції.
(а) - вихідне зображення; (б) $\gamma = 2{,}2$; (в) $\gamma = 0{,}2$

При $\gamma = 1$ характеристика передачі півтонів лінійна, перепади освітленості в тінях і світлі об'єкта відображаються однаково. В разі $\gamma < 1$ деталі на слабо освітлених ділянках стають більш розпізнаваними.

Фільтр Гауса. Є згладжувальним, призначення - придушення шумів, що мають Гаусовий розподіл. В результаті застосування зашумлені пікселі, яскравість яких значно відрізняється від сусідніх, приймають усереднене значення, шум пригнічується, при цьому контури об'єктів підкреслюються, що дуже корисно при розпізнаванні образів на цифрових зображеннях.

В основі фільтра лежить функція Гауса однієї і двох змінних:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}, \quad G(x,y) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2+y^2}{2\sigma^2}}, \tag{2.1}$$

де σ - стандартне відхилення нормального розподілу; x, y - відстані від вихідної точки (пікселя) до точки, для якої підраховується значення функції по вертикалі і горизонталі відповідно;

Рис. 2.4. Результат застосування фільтра Гауса до зашумленого зображення

Медіанний фільтр. У зображеннях використовується переважно для придушення імпульсного шуму. Для кожного пікселя в деякому його оточенні шукається медіанне значення і присвоюється цьому пікселю. Для того щоб знайти медіанне значення пікселя необхідно масив пікселів впорядкувати за їх значенням, і вибрати середній елемент цього масиву, який і буде медіаною.

Значення відновленого зображення при медіанної фільтрації в довільній точці *(x, y)* обчислюється за формулою $f(x,y) = med\{g(s,t)\}$, де (s, t) ∈ S_{xy}.

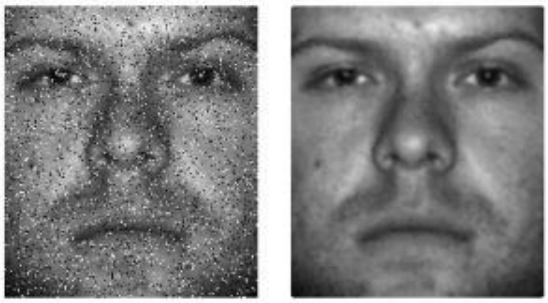

Рис. 2.5. Результат застосування медіанної фільтрації до зашумленого зображення

2.4. Алгоритм ідентифікації користувача в ДС за зображенням особи

Як вже було сказано вище будь-який алгоритм ідентифікації осіб повинен

вирішувати завдання локалізації особи на зображенні, його нормалізації, обчислення ключових ознак і класифікацію. Запропонований в роботі алгоритм розпізнавання осіб в ДС вирішує ці завдання, відміна від базового полягає в тому, що результатом розв'язання задачі локалізації обличчя є координати очей. Виділення обличчя за координатами очей, і його нормалізація виділені в окреме завдання попередньої обробки вхідного зображення [20]. Запропонований алгоритм містить дві основні стадії: навчання та ідентифікація. На обох стадіях попередня обробка зображення особи і обчислення його ключових ознак виконуються за ти самими алгоритмами з однаковими параметрами. Результатом навчання буде набір шаблонів, що описують класи (зареєстровані користувачі), результатом ідентифікації - приналежність вхідного зображення особи до певного класу шляхом порівняння вектора ознаки невідомої особи з вектором ознак осіб з навчальної вибірки.

Завдання попередньої обробки вхідного зображення спрямоване на виділення особи і її геометричне вирівнювання за координатам очей. Точки визначаються вручну на стадії навчання, і додаються у вигляді мета-інформації до зображення. На стадії ідентифікації виявлення особи використовується метод Віоли-Джонса. На етапі попередньої обробки з метою зменшення впливу фактора недостатньої або нерівномірної освітленості застосовується метод гами корекції. Варто зазначити, що для ДС отримання зображення обличчя відвідувача ведеться при неконтрольованих умовах освітленості, і компенсація впливу освітленості на зображенні завдання важлива, від вирішення її залежить точність розпізнавання.

Для обчислення вектора ознак для особи пропонується використовувати метод заснований на ЛБШ. Метод отримав найбільше поширення при вирішенні завдань пов'язаних з розпізнаванням осіб за рахунок своєї простоти, швидкості виконання і інваріантності до освітленості. Також метод має безліч модифікацій, спрямованих на підвищення його ефективності.

Визначення ключових точок особи на зображенні. На даному етапі необхідно вирішити задачу по визначенню точок на зображенні відповідних

центрам очей відвідувача. Координати очей обрані з тієї причини, що за ними можна без особливих труднощів виділити особу на зображенні, масштабувати і повернути в потрібному напрямку. Також аналіз представлених в таблиці 2.1 характеристик зображення особи відвідувача показує, що очі будуть присутні практично на всіх кадрах, отриманих в момент виклику абонента, тому ці точки на зображені можна взяти за основу для виділення особи.

Якщо на стадії навчання при формуванні навчальної вибірки центр очей з допустимою похибкою можна визначити в ручну, то на стадії ідентифікації це необхідно робити методами комп'ютерного зору, тому алгоритм ідентифікації виключає втручання людини в процесі виконання. Для вирішення поставленого завдання, пропонується використовувати один з ефективних методів по локалізації об'єктів на зображенні - метод Віоли-Джонса. Даний метод успішно застосовується для пошуку таких об'єктів на зображенні як лиця, очі, ніс, рот. Перед застосуванням методу необхідно вхідне зображення, отримане з відео, перетворити з кольорового в відтінки сірого. Таке перетворення сприяє зменшенню кількості даних на зображенні. У методі Віоли-Джонса немає необхідності враховувати колір джерел світла, що впливають на сцену і колір шкіри обличчя [16].

Для отримання кольорового зображення у відтінках сірого кольору необхідно виконати перетворення за формулою (2.2):

$$f_{x,y} = \min(255, r_{x,y} \cdot 0{,}3 + g_{x,y} \cdot 0{,}59 + b_{x,y} \cdot 0{,}11) \qquad (2.2)$$

де $r_{x,y}$ - червона компонента; $g_{x,y}$ - зелена компонента; $b_{x,y}$ – синя компонента.

Інтегральне представлення зображень. Інтегральне представлення зображень - це матриця з такими ж розмірами як і вихідні зображення. Кожен елемент містить суму яскравостей пікселів, що знаходяться лівіше і вище даного елемента. Для розрахунку елементів матриці можна скористатися формулою (2.3):

$$L(x,y) = \sum_{i=0,j=0}^{i\leq x, j\leq y} I(i,y) \qquad (2.3)$$

де *I(i,y)* - яскравість пікселя вихідного зображення.

Нехай в зображенні є прямокутник ABCD, наведений на рис. 2.6, тоді інтенсивність пікселів всередині прямокутника D можна виразити через різницю суміжних прямокутників за формулою *S (ABCD) = L(B) + L(D) – L(A) – L(B).*

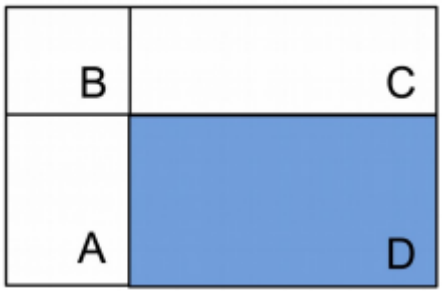

Рис. 2.6. Розрахунок суми яскравостей пікселів в довільному прямокутнику

Ознаки Хаара. Для вікна фіксованого розміру ознаки являють собою множину прямокутних областей білого або чорного кольору (рис. 2.7).

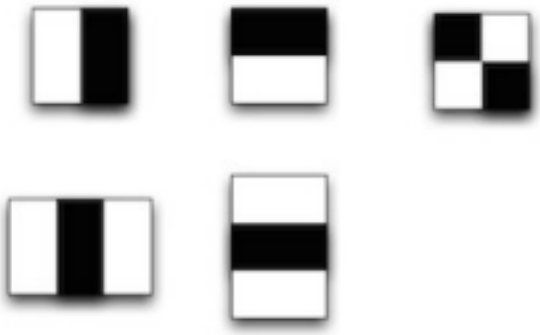

Рис. 2.7. Приклади ознаки Хаара

При обчисленні значень кожної ознаки Хаара, сумуючи значення всіх необхідних пікселів досліджуваної області, буде виконуватися *m·n* операцій, де *n* і *m* - ширина і висота досліджуваної області відповідно, що потребує значних

обчислювальних ресурсів. Використання інтегрального представлення зображення описаного вище дозволяє знизити витрати на обчислювальні ресурси.

Бустінг. Бустінг над деревами, які вирішують задачу, є одним з найбільш ефективних методів щодо якості класифікації. Подальшим розвитком є розробка більш досконалого сімейства алгоритмів бустінга AdaBoost, представлена в 1997 р. Йоав Фройндом (Freund) і Робертом Шапіро (Schapiro) [23].

Використання каскадів ознак. Каскад застосовується до зображення за такими правилами: робота з «простими» класифікаторами - при цьому відкидається частина «негативних» вікон; позитивне значення першого класифікатора запускає другий, більш пристосований і так далі; негативне значення класифікатора на будь-якому етапі призводить до негайного переходу до наступного скануючого вікна, старе вікно відкидається; ланцюжок класифікаторів стає складнішим, тому помилок стає набагато менше.

Навчання класифікатора Віоли-Джонса. Для навчання класифікатора Віоли-Джонса необхідно побудувати навчальну множину із зображень, котрі містять обличчя або очі і зображень, котрі їх не містять. Для стабільно працюючого детектора обличь необхідно порядка 3000-4000 позитивних прикладів і стільки ж негативних. Навчання класифікатора досить тривала процедура, так як для знаходження найбільш оптимальних значень ознак необхідно застосувати весь їх набір до усієї множини зображень. Процес навчання може займати до декількох днів, але саме виділення об'єкта на зображенні виконується досить швидко (десятки мілісекунд), що дозволяє використовувати даний метод в реальному часі.

Для визначення ключових точок, в першу чергу на вхід навченого на знаходження особи алгоритму, подається один з кадрів відео користувача, отриманого з ПВ в момент виклику абонента. Якщо результат позитивний і була знайдена особа на зображенні, то алгоритм поверне координати відповідної йому прямокутної області. Далі до виділеної області застосовується вже алгоритм, навчений на визначення очей. Аналогічно відбувається визначення координат точок, відповідних центрам очей відвідувача. Так на виході детектора будуть

визначені координати точок, відповідних положенням очей, за якими можна однозначно виділити обличчя. Разом з вхідним зображенням ці значення передаються на етап попередньої обробки, де відбувається безпосередньо виділення самого обличчя і приведення його до певного канонічного вигляду.

Виділення та попередня обробка зображення обличчя. Перша задача, яку необхідно вирішити на даному етапі - це поворот зображення таким чином, щоб очі знаходилися на одній горизонтальній лінії. Зображення є матрицею, застосувавши афінне перетворення відповідне повороту зображення на кут α з центром обертання в точці, рівній розташуванню правого ока. Кут повороту в градусах розраховується за формулою:

$$\alpha = arctg\frac{y_2 - y_1}{x_2 - x_1} \cdot \frac{180}{\pi}, \quad (2.4)$$

де x_1, y_1 - координати правого ока; x_2, y_2 - координати лівого ока;

Далі вирішується задача по визначенню області відповідної обличчю на зображенні. Виділити необхідно таку область, яка б містила мінімальну кількість зовнішніх факторів, що не відносяться до особи людини і одночасно дозволяла б ідентифікувати особу. На рис. 2.8 відображені основні відстані щодо розташування очей, котрі дозволяють визначити таку область.

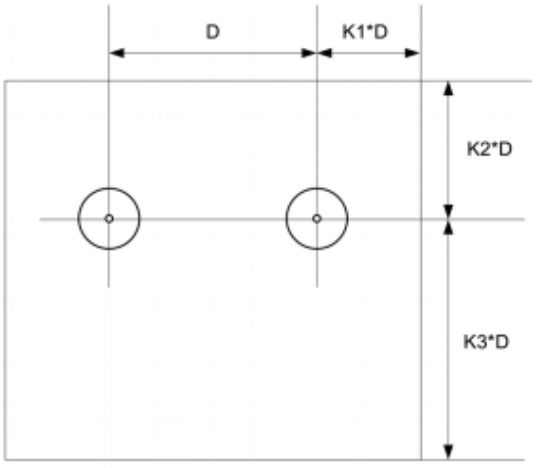

Рис. 2.8. Область обличчя, виділена по розташуванню очей на зображенні

Розташування лівого верхнього кута прямокутника в системі координат зображення можна обчислити таким чином $x = x_1 - k_1 \cdot D$, $y = y_1 - k_2 \cdot D$. Ширину і висоту як $w = k_1 \cdot D \cdot 2 + D$, $h = k_2 \cdot D + k_3 \cdot D$.

Тут D - відстань між очима в оригінальному документі визначається за формулою:

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}, \quad (2.5)$$

де k_1, k_2, k_3 - коефіцієнти, які визначають корисну область обличчя, визначають емпірично, спочатку приймемо рівними $k_1 = 0.5$, $k_2 =$ 0.33, $k_3 = 1.38$.

Після обчислення координат необхідно виконати перевірку, що виділена область знаходиться в межах зображення, Тобто x, y не повинні мати від'ємні значення, а $x+w$, $y+h$ бути більші, ніж ширина і висота вхідного зображення відповідно, якщо умови виконуються, виділяємо область в окреме зображення, в противному випадку вважаємо, що обличчя не визначена.

Отримане зображення обличчя необхідно масштабувати таким чином, щоб фінальна ширина і висота були рівні якійсь постійній величині. При цьому величину потрібно підбирати з урахуванням того, щоб не доводилося занадто сильно стискати або збільшувати зображення. Все залежить від характеристик відеокамери, яка знімає відвідувача, для характеристики наведених в таблиці 2.1, можна визначити ширину і висоту таким чином $w = 144$, $h = 144 \cdot (k_1 + k_2)$.

Для компенсації нерівномірного освітлення пропонується використовувати метод гами корекції за формулою (2.1). З тієї причини, що обличчя отримані в кадрах відео, можуть мати досить сильні нелінійні засвітки, вирівнювання гістограм може тільки погіршити результат, тому даний метод не використовується.

Обчислення вектора ознак. В основі алгоритму обчислення ключових ознак в роботі пропонується використовувати розширений оператор ЛБШ. Використання кругового околу і білінійної інтерполяції значень інтенсивностей

пікселів дозволяє побудувати ЛБШ з довільною кількістю точок *P* і радіусом *R*, приклади зображені на рис. 2.9.

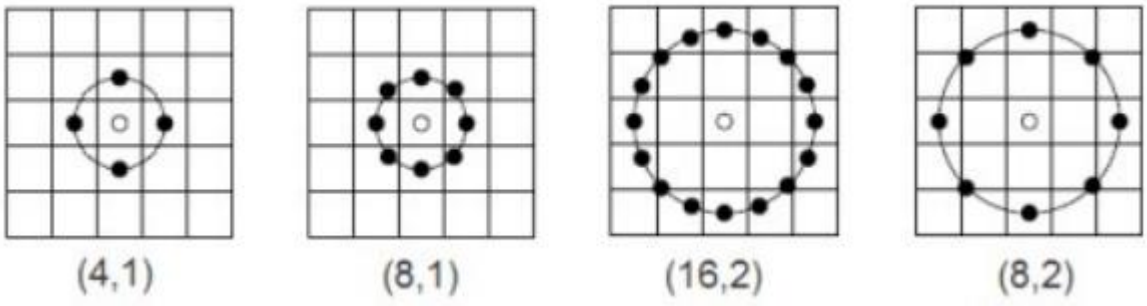

Рис. 2.9. Розширений оператор ЛБШ

Найбільш важливу для класифікації інформацію містять рівномірні ЛБШ. До таких відносяться шаблони, які містять не більше трьох серій «0» і «1», шаблони представлені в табл. 2.2. Так як саме вони кодують кінці ліній, кути, плями і інші особливості зображення, також вони забезпечують істотну економію пам'яті, *P (P-1) +2* різних шаблонів замість *2P*.

Таблиця 2.2

Приклад рівномірних і нерівномірних ЛБШ

ЛБШ	Кількість серій	Рівномірний
11111111	1	так
00001111	2	так
01110000	3	так
11001110	4	ні
11001001	5	ні

В результаті застосування ЛБШ з кількістю точок 8, радіусом 2 і не більше трьох серій «0» і «1» ($LBP^{u2}_{(8.2)}$) до зображення

розміром 144x123 підсумкове зображення буде меншого розміру 140x119, так як два пікселя з кожного боку потрібно для того, щоб обчислити ЛБШ в самій крайній точці зображення.

Для більш ефективного опису зображення обличчя його необхідно розбити на області і далі для кожної побудувати гістограму. Беручи до уваги, що зображення може складатися з m регіонів R_0, R_1, ..., R_{m-1}, тоді гістограма буде розраховується для кожного регіону, в нашому випадку загальна кількість регіонів 49. Приклад зображений на рис. 2.10. Гістограма для кожного регіону зображення $f_l(x,y)$ обчислюється за формулою (2.6):

$$H_i = \sum_{x,y} I\{f_l(x,y) = i\}, i = 0,\dots,n-1, \tag{2.6}$$

де n - число різних обчислених значень оператора ЛБШ в регіоні; $I(A) = \begin{cases} 1, & A \text{ is true} \\ 0, & A \text{ is false} \end{cases}$

Потім отримані гістограми об'єднуються в одну [24]. Це дозволяє отримати інформацію не тільки про наявність тих чи інших локальних особливостей, а й про місце їх розташування на зображенні. Розрахуємо гістограму за формулою:

$$H_{i,j} = \sum_{x,y} I\{f_l(x,y = i) I\{x,y\} \in R_j\}, i = 0,\dots,n-1, j = 0,\dots,m-1. \tag{2.7}$$

Рис. 2.10. Приклад зображення особи з обчисленими шаблонами $LBP^{u2}_{(8.2)}$, розбите на області 7x7

В результаті отримаємо вектор розмірністю 2891 (всього 7x7 регіонів і для кожного обчислена гістограма 59 bin), який і буде описувати ключові особливості зображення обличчя (див. рис. 2.10).

Навчання. Процес навчання зводиться до формування єдиного списку векторів ознак осіб з навчальної вибірки. Кожному вектору зіставляється ідентифікатор зареєстрованого в системі користувача, за зображенням обличчя якого і був обчислений даний вектор.

Ідентифікація. Завдання ідентифікації зводиться до зіставлення вхідного зображення особи з відомими зображеннями осіб з тренувального набору. Якщо невідомій особі з заданою ймовірністю відповідає особа з відомих вважається, що особа ідентифікована. Для порівняння двох осіб необхідно вирахувати відстань між векторами ознак, отриманих для їх зображень. Для цього порівнюється гістограма невідомої особи, обчислена за формулою (2.8), з кожної з гістограм навчальної вибірки. Часто для цього обчислюється відстань Хі-квадрат [24], тоді відстань між моделями буде визначається за формулою:

$$\chi^2(S,M) = \sum_i \frac{(S_i - M_i)^2}{|S_i + M_i|} \tag{2.8}$$

де S - вектор ознак невідомої особи; M - вектор ознак, отриманий для відомого зображення особи.

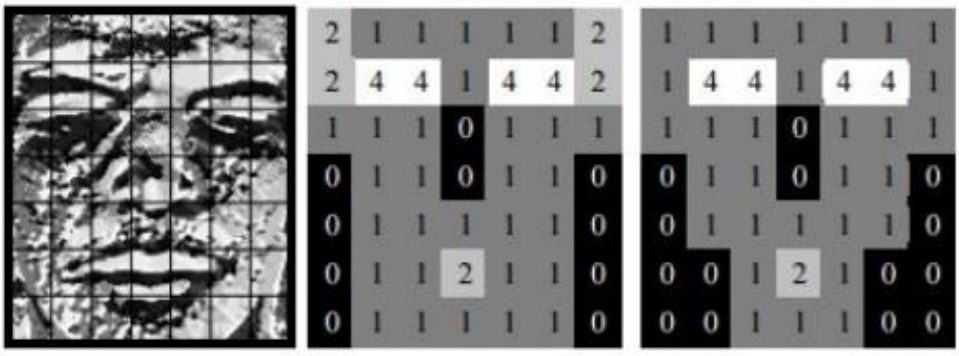

Рис.2.11. Приклад зображення обличчя і ваги його областей

Деякі ділянки вихідного зображення можуть нести важливішу інформацію, ніж інші, наприклад, область очей, носа, рота. Для акцентування таких ділянок їм присвоюються ваги.

Відстань з урахуванням ваг областей обчислюється за формулою (2.9):

$$\chi_w^2(S,M) = \Sigma_{i,j} w_j \frac{(S_{i,j}-M_{i,j})^2}{|S_{i,j}+M_{i,j}|} \quad (2.9)$$

де w_j - вага області *i*.

2.5. Висновки до розділу

В цьому розділі проаналізовані основні методи розпізнавання за зображенням особи. Описані задачі розпізнавання осіб на зображеннях і методи їх вирішення (детектування особи на зображенні, нормалізація зображення обличчя, обчислення ключових ознак і зіставлення з еталоном). Наведено особливості методів підвищення точності алгоритмів розпізнавання зображення особи. Докладно описано алгоритм ідентифікації користувача в ДС за зображенням особи. Запропонований алгоритм містить дві основні стадії: навчання та ідентифікація. На обох стадіях попередня обробка зображення особи і обчислення його ключових ознак виконуються за ти самими алгоритмами з однаковими параметрами. Результатом навчання буде набір шаблонів, що описують класи (зареєстровані користувачі), результатом ідентифікації - приналежність вхідного зображення особи до певного класу шляхом порівняння вектора ознаки невідомої особи з вектором ознак осіб з навчальної вибірки.

РОЗДІЛ 3
ПРАКТИЧНА ЧАСТИНА

3.1. Опис архітектури . Загальна структура системи

ДС, котрі базуються на IP технологіях, дозволяють фіксувати відео зображення відвідувача засобами вбудованої в ПВ відеокамери, можуть бути розширені функцією автоматичного розпізнавання відвідувача за рахунок підключення в їх мережу додаткового МРВ, як показано на рис. 3.1.

МРВ є якимось обчислювальним ресурсом у вигляді одного або декількох процесорів, деякого обсягу постійної і оперативної пам'яті, що в сукупності дозволяє виконувати на ньому програми.

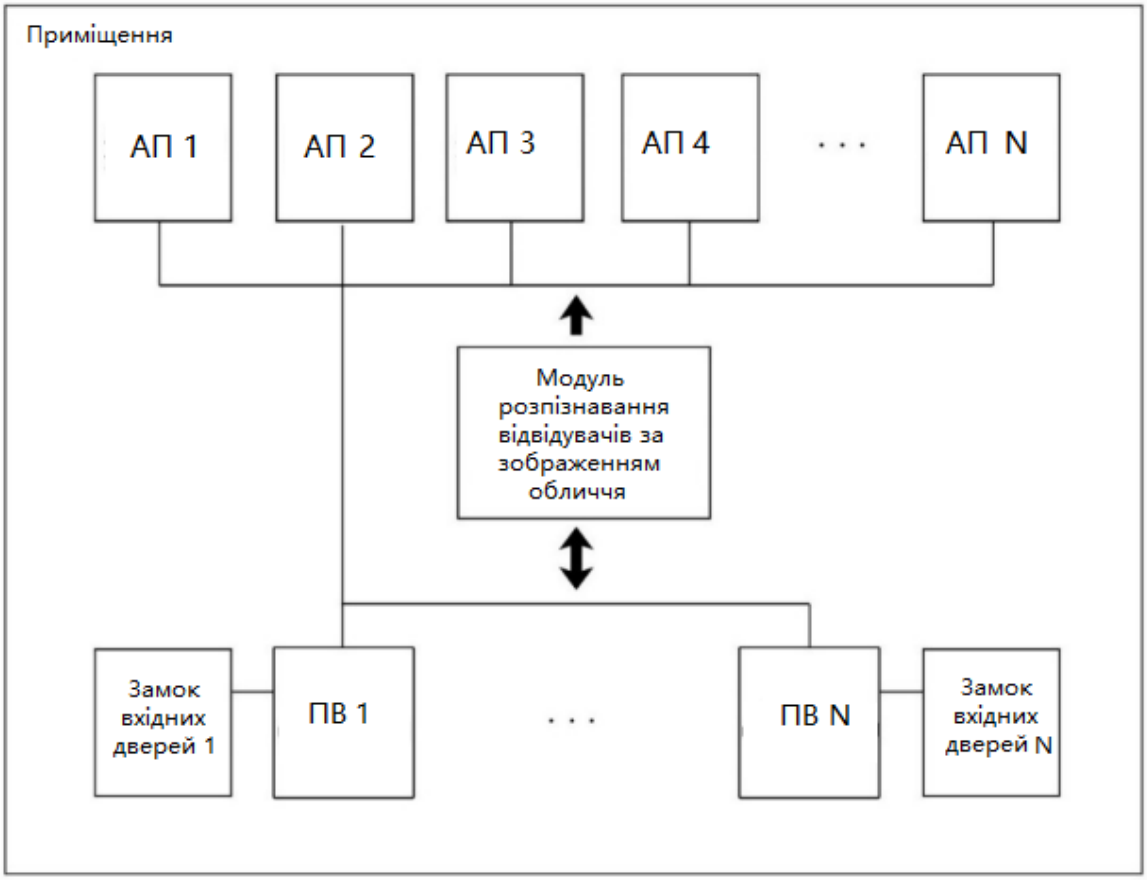

Рис. 3.1. Загальна структура системи із застосуванням МРВ

Таким пристроєм може бути однокристальна ЕОМ з мережевим інтерфейсом Ethernet. МРВ крім програми, що реалізує алгоритм розпізнавання відвідувача за зображенням особи, містить базу зображень осіб, котра утворює тренувальну вибірку, журнал доступу і Web API для взаємодії користувача з модулем через інші компоненти ДС (ПВ, АП). Розміщення необхідних програмних компонент на окремому пристрої дозволяє виконувати його інтеграцію в ДС з різною кількістю абонентів і контрольованих входів в приміщення. Розширення системи і заміна застарірил чи тих, що вийшли з ладу компонентів (ПВ, АП) також може бути виконана зі збереженням стану функції автоматичного розпізнавання користувача.

При інтеграції МРВ в ДС логіка роботи останнього буде частково змінена. МРВ в залежності конфігурації, перехоплює виклик абонента з ПВ і робить аналіз отриманого відео зображення відвідувача. Якщо особа відвідувача ідентифікована, і їй дозволено доступ в приміщення, МРВ приймає рішення про відкриття дверей і відправляє відповідну команду до ПВ, тобто певним чином емулює натиснення кнопки відкриття дверей на АП.

У разі закритого доступу для ідентифікованої особи, оповіщає її методом передачі відповідного звукового сигналу до ПВ на відтворення. При неможливості ідентифікувати особу відвідувача, МРВ переадресовує виклик на АП і подальша робота системи буде виконується за стандартними сценаріями типової ДС.

Конфігурація модуля, що включає реєстрацію нових відвідувачів, налаштування індивідуального рівня доступу, збільшення обсягу тренувальної вибірки осіб, виконується адміністратором через ПК, під’єднаний в домофонну мережу або абонентом через АП, якщо останній не підтримує необхідний функціонал, то використовується ПК, аналогічно до адміністратора.

3.2. Визначення вимог до системи

Для специфікації функціональних вимог до системи використовується діаграма прецедентів, наведена на рис. 3.2. Актори на діаграмі: відвідувач, в інтересі якого отримати доступ в приміщення, абонент і адміністратор виконує необхідне налаштування системи.

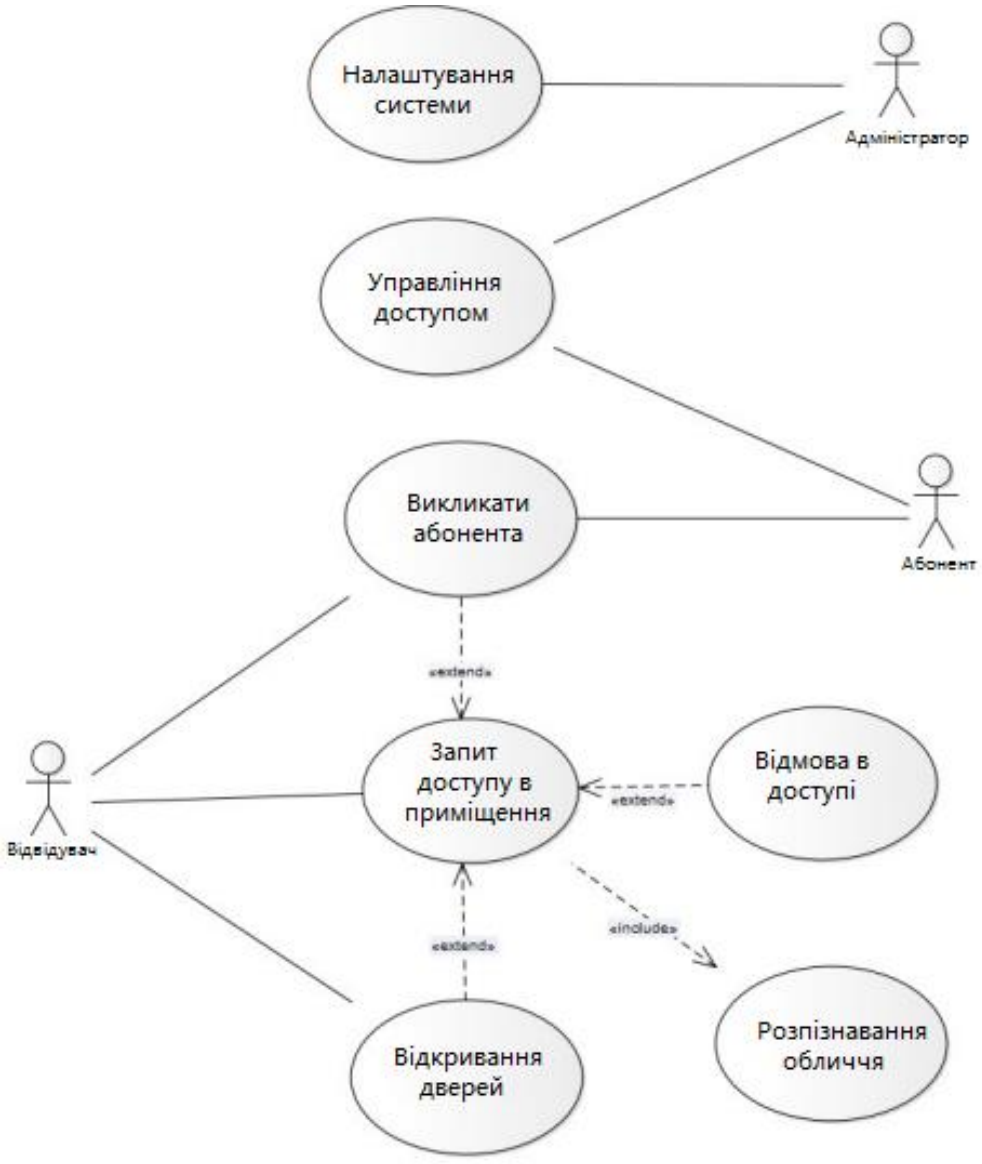

Рис. 3.2. Діаграма прецедентів ДС

Кожен з акторів взаємодіє з системою за рахунок ініціалізації варіанта використання. Як варіанти використання визначені: налаштування системи, управління доступом і запит доступу в приміщення. Останній включає в себе розпізнавання особи і в залежності від його результату може бути розширений варіантами викликів абонента, відмовою в доступі або відкриття дверей.

Варіанти використання можуть бути доповнені діаграмами діяльності UML. Діаграми даного виду дозволяє визначити поведінку за рахунок послідовного виконання поведінок більш низького рівня і зображені на рис. 3.3 і 3.4.

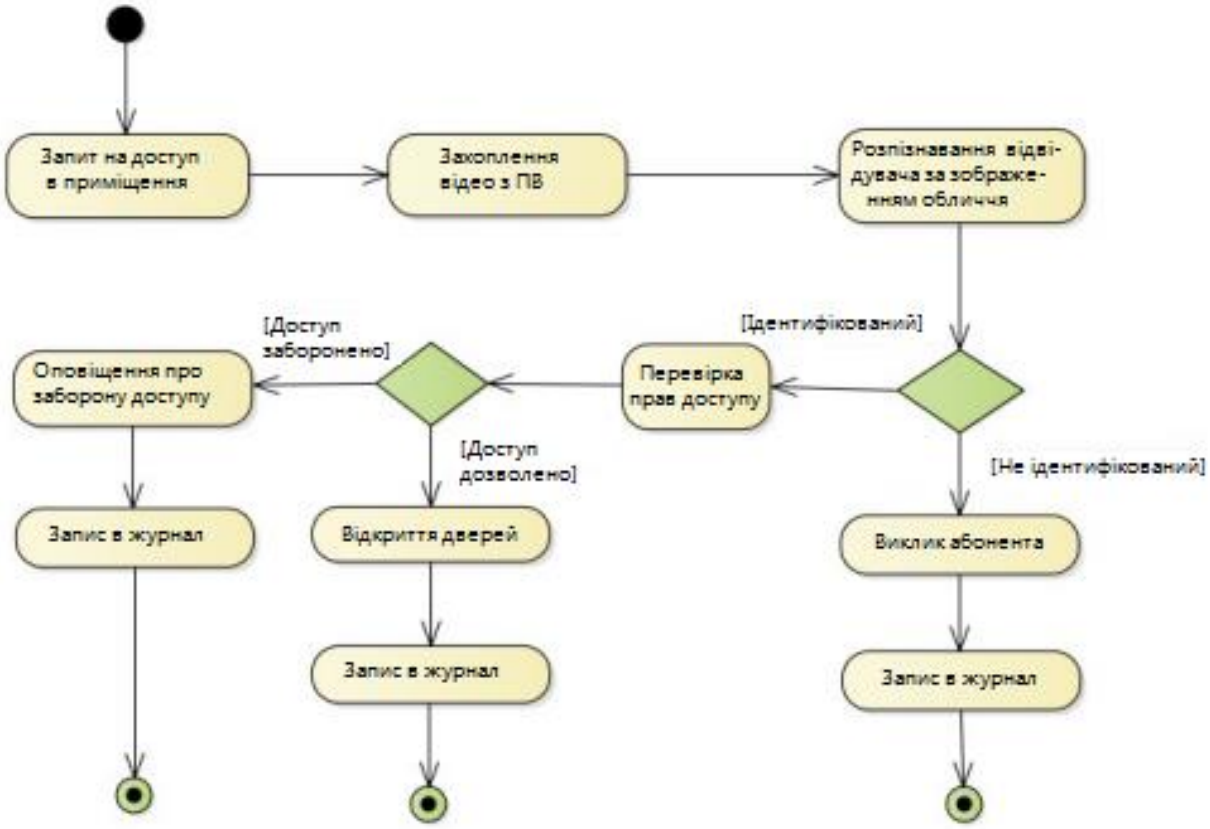

Рис. 3.3. Діаграма діяльності для прецеденту «Запит доступу в приміщення»

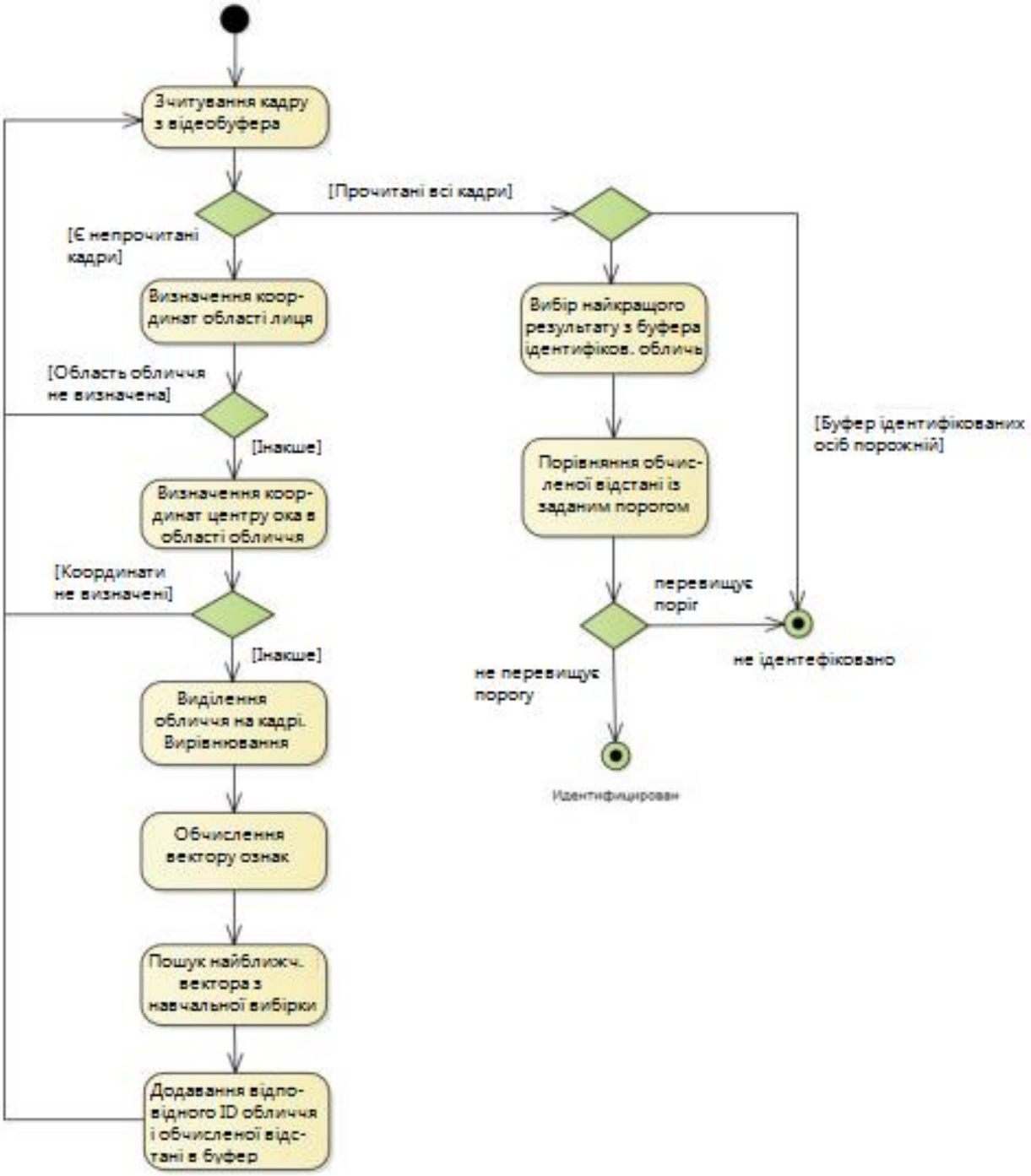

Рис. 3.4.Діаграма діяльності для прецеденту «Розпізнавання обличчя»

3.3. Розгортання системи

Проектована система відноситься до типу вбудованих, діаграма розвертання для якої зображена на рис. 3.5. Вузли системи, крім контролера замка дверей,

підключені до локальної мережі, сам контролер підключається безпосередньо до ПВ. Вузли, відповідні АП і ПВ, є стандартними пристроями ДС та використовують для взаємодії між собою стек протоколів TCP / IP. На робочій станції адміністратора розгортається локальне клієнтське ПЗ (Web-browser) з одним із поширених веб-браузерів Chrome, Opera, Firefox або Inernet Explorer.

На вузлі, який виконує функцію розпізнавання користувача за зображенням обличчя, розгортаються такі компоненти:

– IdentVisitor - реалізує алгоритм розпізнавання користувача по зображенню особи і взаємодіє з ПВ і АП системи для організації автоматизованого доступу в приміщення;

– FaceDB - містить БД осіб відвідувачів;

– AccessLog - реєстрація успішних і неуспішних спроб доступу в приміщення;

– WebApi - інтерфейс для взаємодії з вузлом по протоколу HTTP.

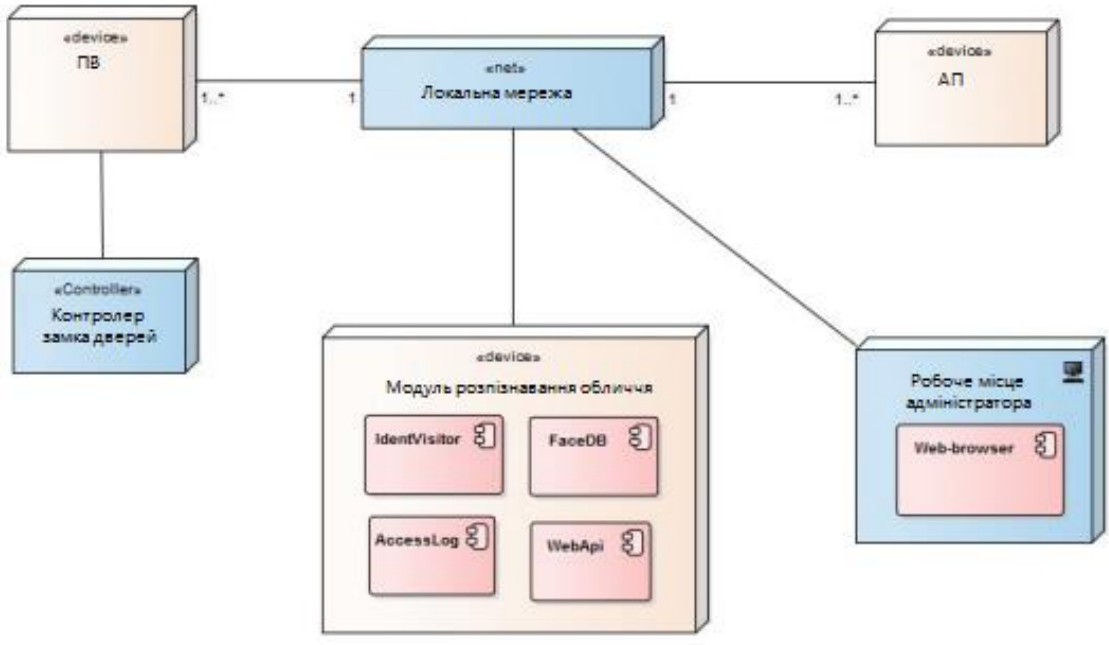

Рис. 3.5. Діаграма розгортання

3.4. ПЗ

3.4.1 Опис і характеристики

Розроблена в даній роботі програма реалізує алгоритм, котрий відподіває діаграмі діяльності, зображеній на рис. 3.4. Програмна реалізація алгоритму взаємодії з вузлами системи зображеного на рис. 3.5 буде залежати від специфіки самих пристроїв і в більшості випадків буде грунтуватися на стандартних компонентах роботи з протоколами RTSP, RTP, HTTP, SIP та в даній роботі на розглядається.

Програма складається з чотирьох модулів, ієрархія яких приведена на рис. 3.6. Кожен модуль містить певний набір функцій для вирішення поставлених завдань. Перелік функцій і їх призначення наведені в додатку Б. Як мова програмування для реалізації алгоритму була обрана C ++. Визначення координат області особи і центру очей на зображенні реалізовано із застосуванням сторонньої бібліотеки OpenCV. Бібліотека містить реалізацію методу Віоли-Джонса з навченими класифікаторами на визначення осіб і очей на зображенні.

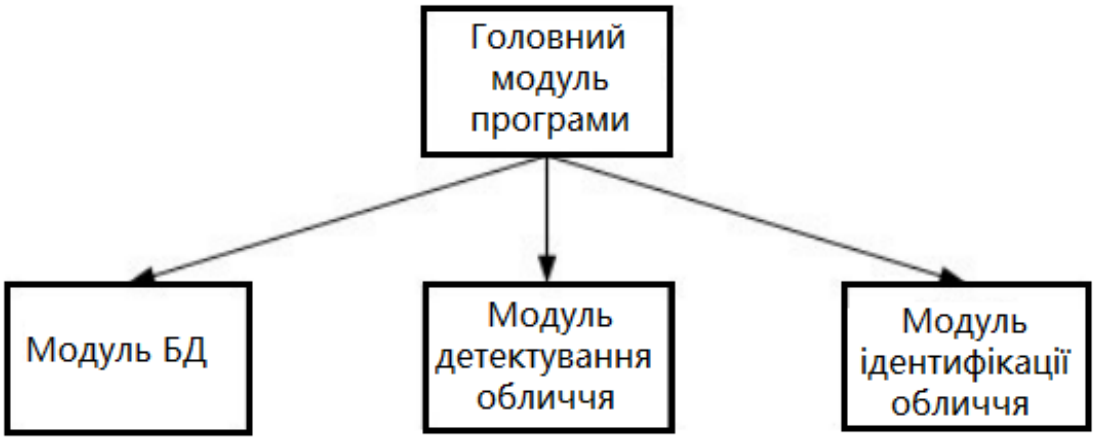

Рис. 3.6. Ієрархія модулів програми

Реалізація програми була виконана в середовищі розробки Microsoft Visual Studio і є консольним додатком. Він читає директорію з відеофайлами, кожен з яких містить запис одного відвідувача в момент виклику абонента, ідентифікує його особу і записує результат в текстовий файл, аналіз якого в подальшому може зробити висновки про ефективність обраного алгоритму. характеристики додатка наведені в таблиці 3.1.

Компіляція вихідних кодів програми в динамічну або статичну бібліотеку дозволить використовувати її для написання інших програм, які реалізують алгоритм взаємодії з вузлами конкретної системи.

Таблиця 3.1

Характеристики програми

Характеристика	Значення
Кількість модулів	4
Кількість рядків коду	1413
Кількість функцій	19
Бібліотеки, що використовуються	OpenCV 3.1.0
Операційна система	Windows
Розмір вихідних кодів	40 949 байт
Розмір виконавчого файлу	82 434 байт
Необхідний об'єм оперативної пам'яті	150 – 200 МБ для відеофрагментів транзакцій з роздільною здатністю 960 x 576, тривалістю 6-10 с, частотою 25 – 30 к/с
Архітектура процесора	X86

3.4.2. Приклад роботи

Перед першим запуском програми необхідно сформувати навчальну вибірку. Це можна зробити вручну або за допомогою веб-інтерфейсу. Для

формування вибірки вручну необхідно в директорії додатка \database \ training_set\ для кожного користувача створити піддиректорію з ім'ям його ID. Кожна така директорія повинна містити набір зображень особи користувача, отриманих з відео камери в ракурсі анфас в форматі jpg. Структура директорії навчальної вибірки наведена на рис. 3.7. У файлі index необхідно описати кожне зображення особи, для це за допомогою текстового редактора через крапку з комою для кожного зображення перерахувати з нового рядка, дотримуючись порядку, наступні параметри: ім'я зображення; координата *x* правого ока; координата *y* правого ока; координата *x* лівого ока; координата *y* лівого ока; номер транзакції, з якої отримано кадр (0 якщо немає транзакції); прапорець, який позначає чи застосовувати дане зображення при навчанні алгоритму чи ні (0 - так, 1 - немає).

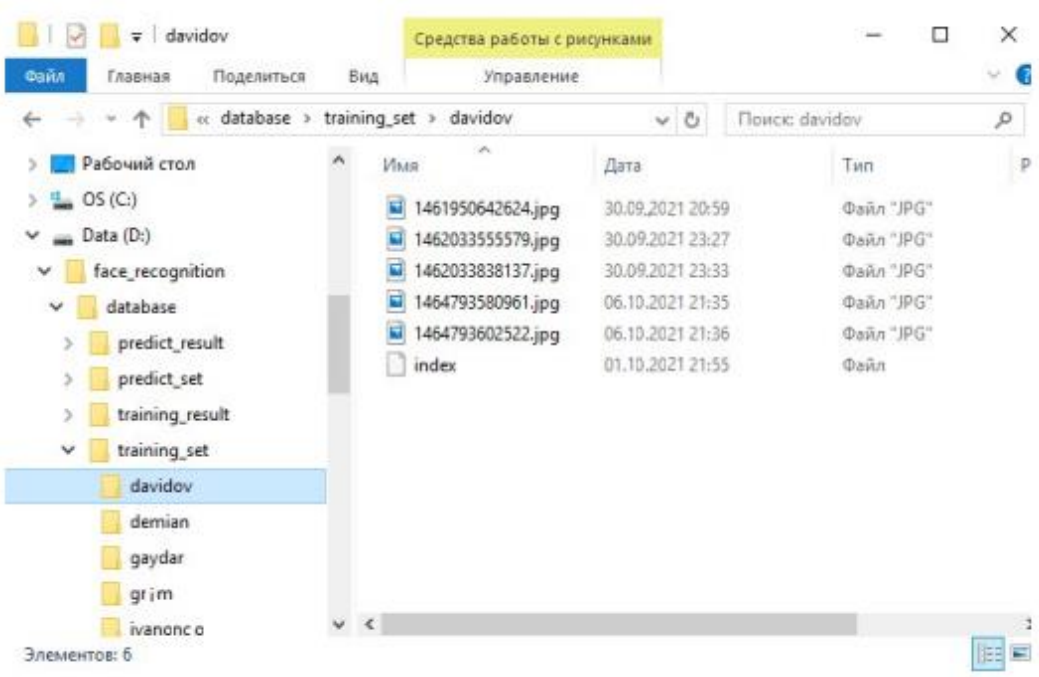

Рис. 3.7. Структура директорії training_set

Наступний крок - формування тестової вибірки. Процес аналогічний до формування навчальної вибірки. В директорії \ database \ predict_set \ необхідно створити піддиректорії користувачів, які містять відеофрагменти транзакцій.

Відео- файли повинні бути в контейнері avi і називатися відповідно до номера транзакції. Структура директорії приведена на рис. 3.8.

Для запуску програми необхідно в командному рядку запустити виконати файл programm.exe. Першим аргументом вказується ID користувача з тестової вибірки, другим - номер транзакції. В результаті розпізнавання буде виведений ID особи з навчальної вибірки, якому з більшою часткою ймовірності відповідає користувач на тестовому відео фрагменті.

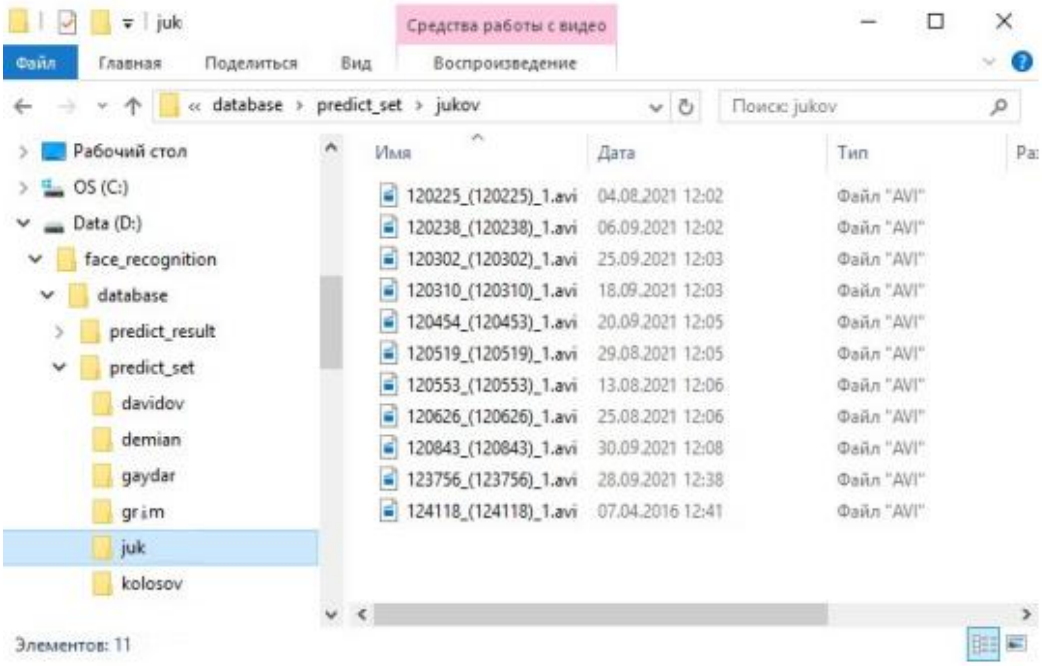

Рис. 3.8. Структура директорії predict_set

Навчання алгоритму виконується перед ідентифікацією в момент запуску, окремо запускати програму на навчання не потрібно. Для ідентифікації користувачів, які незареєстровані в навчальній вибірці, необхідно задати оптимальне значення порога, параметр threshold в файлі config.txt. Результат роботи програми наведено на рис. 3.9.

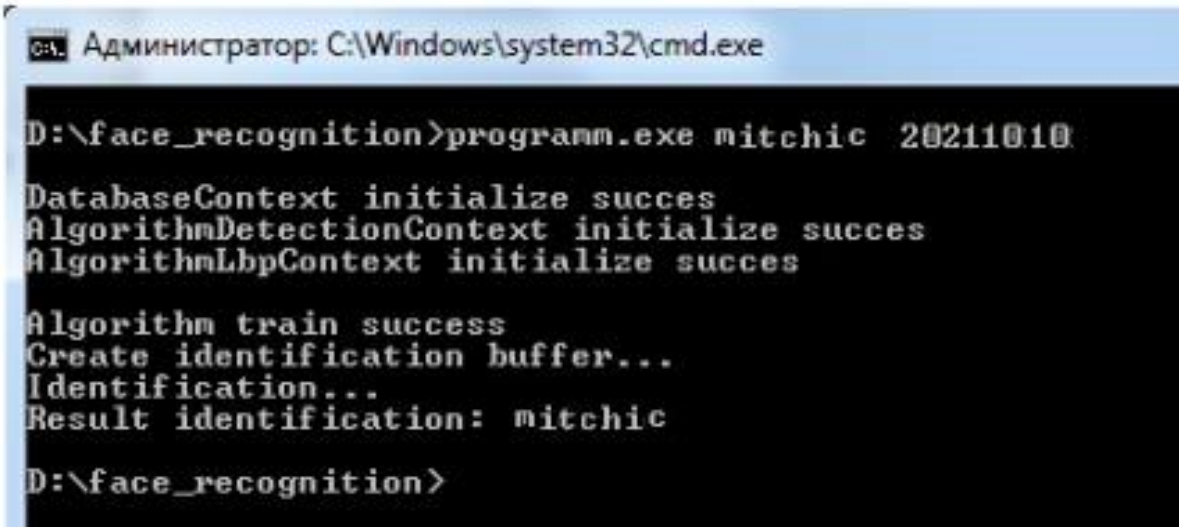

Рис. 3.9. Виконання programm.exe в командному рядку

При запуску без аргументів додаток виконує послідовну ідентифікацію кожної транзакції з тестової вибірки, результат крім виводу на екран фіксується в директорії \ database \ predict_result \ у вигляді зображень і текстових файлів.

Для більш детального аналізу результату роботи алгоритму, що актуально при великих обсягах вибірок, можна скористатися веб-інтерфейсом.

3.5. Результати випробувань

Для тестування програми використовувалася одноабонентська ПВ з параметрами, наведеними в табл. 3.2. Панель була встановлена на вході в приміщення і обмежувала доступ для 15 осіб (справжні обличчя).

Експлуатація проводилася при різних умовах освітленості. У темний час доби ПВ виконувала відеозйомку з включеним ІЧ-підсвічуванням. Протягом двох тижнів велася відео фіксація кожного відвідувача за 3 секунд до натискання кнопки виклику абонента і 3 секунд після. В результаті було отримано 250 відео фрагментів (транзакцій), тривалістю по 6 секунд кожен. Розподіл відвідувачів по транзакціях наступний: 20 невідомих осіб і 230 справжніх осіб приблизно з

однаковим розподілом. Для навчання алгоритму було відібрано по 5 транзакцій для кожного справжнього обличчя що в цілому склало 75 шаблонів осіб.

Таблиця 3.2

Параметри ПВ

Найменування	Значення
Роздільна здатність відео	960 x 576
Частота кадрів	25
Чутливість	0,1 лк (день) / 0,01 лк (ніч) / 0 лк (при ввімкненій підсвітці)
Об'єктив	3,7 мм, F 2.0
Кут огляду	65 ° (по горизонталі), 51 ° (по вертикалі)
Шумопридушення	2DNR
Підсвітка	ІЧ-світлодіоди

Решта транзакцій використовувалися для тестування алгоритму. Так як загальна кількість транзакцій містить відомі і невідомі особи, то така множина ідентифікації відноситься до відкритої. Експлуатаційні характеристики біометричної системи ідентифікації на відкритій множині можуть бути зображені у вигляді кривої, котра показує залежність ймовірності істинно позитивної ідентифікації від ІХПІ при варіюванні порога вирішального правила [25].

Криві залежності ймовірності ідентифікації зображені на рис. 3.10 і 3.11. Кожна крива на рис. 3.10 відповідає певній кількості шаблонів обличь для кожної зареєстрованої особи.

Імовірність ідентифікації - частка транзакцій ідентифікації користувачів, зареєстрованих в системі, для яких визначено правильний ідентифікатор.

ІХПІ - частка транзакцій ідентифікації користувачів, які не зареєстровані в системі, для яких визначено ідентифікатор зареєстрованого користувача.

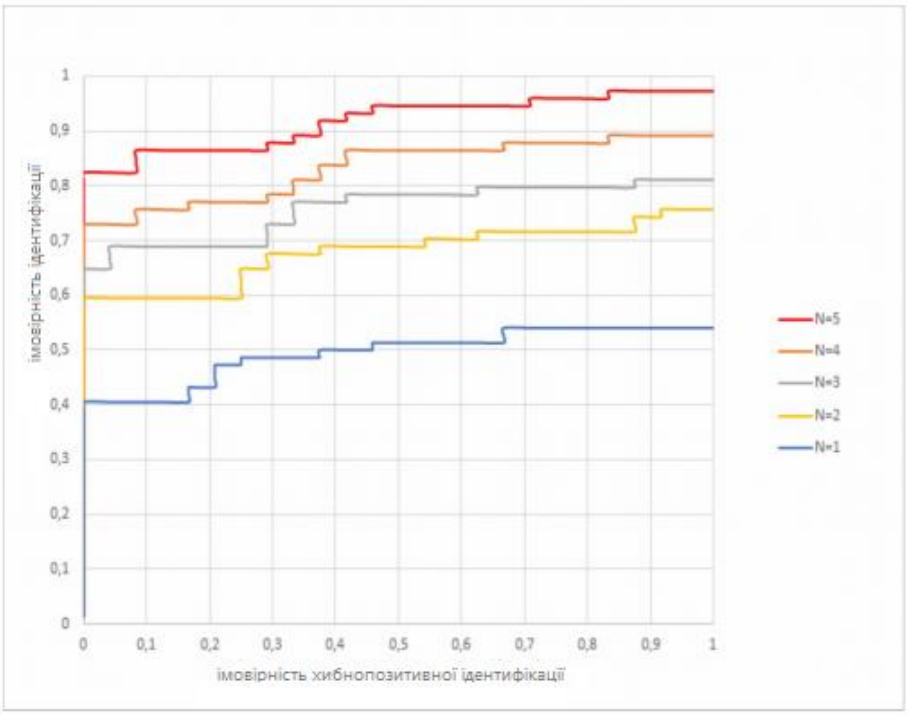

Рис. 3.10. Залежність ймовірності істинно позитивної ідентифікації від хибно позитивної, де N - кількість шаблонів обличь для кожної особи

На рис. 3.11 наведені криві для випадків верифікації та ідентифікації.

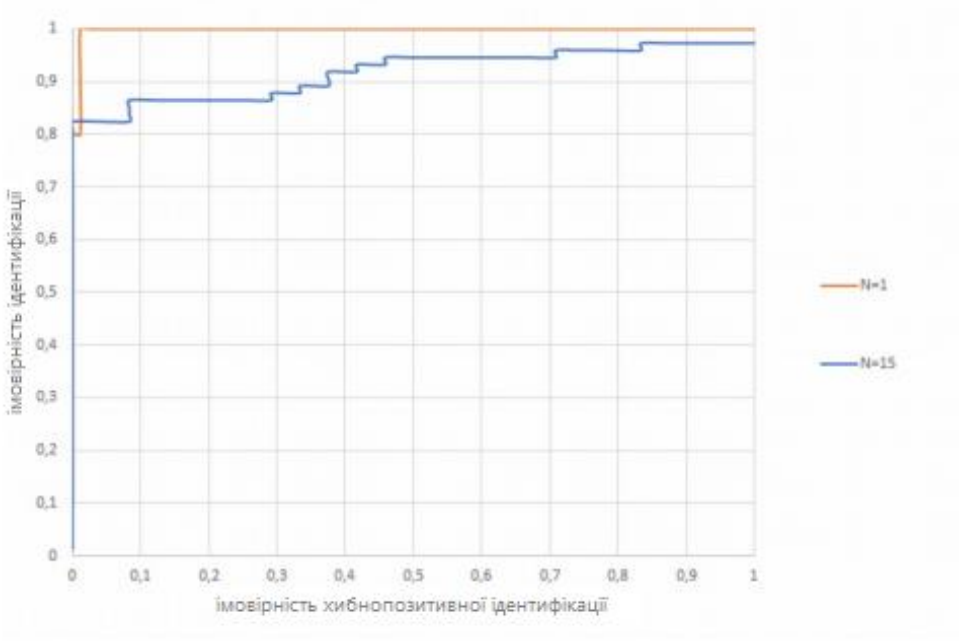

Рис. 3.11. Залежність ймовірності істинно позитивної ідентифікації від хибно позитивної, де N - кількість зареєстрованих осіб

Аналіз наведених вище результатів показує, що збільшення кількості шаблонів обличь для кожного зареєстрованого відвідувача збільшує ймовірність того, що він буде вірно розпізнаний програмою. Також на точність розпізнавання впливає кількість зареєстрованих осіб. Якщо в БД зареєструвати одну персону, то ймовірність її ідентифікації досягає максимальних значень при прийнятному значенні ІХПІ. Таким чином в режимі верифікації розпізнавання відвідувачів виконується з більшою точністю. У табл. 3.3 наведені кількісні характеристики алгоритму розпізнавання.

Таблиця 3.3

Точність розпізнавання при різних значеннях ІХПІ і обсягу бази зареєстрованих осіб N

ІХПІ	N=1 (верифікація)	N=15 (ідентифікація)
0	80 %	82 %
0,02	99 %	82 %

3.6. Висновки до розділу

Для програмної реалізації алгоритму ідентифікації була обрана С ++, середовище розробки Microsoft Visual Studio. Визначення координат області особи і центру очей на зображенні реалізовано із застосуванням сторонньої бібліотеки OpenCV.

Отримані в цьому розділі результати показують, що збільшення кількості шаблонів обличь для кожного зареєстрованого відвідувача збільшує ймовірність того, що він буде вірно розпізнаний програмою. Також на точність розпізнавання впливає кількість зареєстрованих осіб. В режимі верифікації розпізнавання відвідувачів виконується з більшою точністю.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є підвищення ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп’ютерної техніки, зокрема ПК та периферійних пристроїв, то обов’язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки ПЗ комп’ютерних систем, в тому числі і фахівців з підвищення ефективності контролю доступу в приміщення, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [30]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог;

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу

провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування

ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА.

4.2. Функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу

Моніторинг довкілля – це система спостереження, збирання та аналізу інформації про ситуацію, що може скластись під час надзвичайних ситуацій мирного та воєнного часу. Також це система спостереження за визначеними об'єктами, явищами та процесами з метою оперативного оцінювання їх стану, виявлення результатів впливу на них зовнішніх чинників та прийняття відповідних управлінських рішень (ДСТУ 3891:2013) (див. ДСТУ 7295:2013).

Моніторинг потенційно небезпечних об'єктів це спостереження, контролювання за зміною параметрів технологічних режимів з метою збирання, збереження, передавання та аналізування інформації щодо поточного стану потенційно небезпечних об'єктів, наявності та кількості порушень вимог безпеки, відпрацювання рекомендацій щодо проведення 98 робіт із запобігання та

ліквідування техногенних надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг джерел надзвичайних ситуацій це система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації стосовно стану об’єктів моніторингу та розроблення науково-обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування надзвичайних ситуацій (ДСТУ 7295:2013).

Моніторинг довкілля – це систематичні спостереження і контролювання, які проводять регулярно, за єдиною програмою для оцінювання стану довкілля, аналізування процесів, які відбуваються в ньому і своєчасне виявлення тенденцій його змінювання (ДСТУ 7295:2013).

Моніторинг надзвичайних ситуацій (НС) – система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації щодо об’єктів моніторингу та розроблення науково обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування НС.

Моніторинг небезпечних явищ та процесів це система спостереження та контролювання за розвитком небезпечних та стихійних природних явищ і процесів, чинниками, які спричинюють їх формування та розвиток, аналізування, збереження та передавання інформації щодо виявлення тенденцій їх змінювання, розроблення комплексу заходів щодо запобігання природним надзвичайним ситуаціям та ліквідування їх наслідків. Небезпечні природні явища і процеси підрозділяють на геофізичні, геологічні, гідрологічні, метеорологічні, медико-біологічні та пожежі в природних екосистемах (ДСТУ 7295:2013).

Моніторинг пожеж в екосистемах це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо 99 пожежної небезпеки в природних екосистемах (умов погоди, стану горючих матеріалів, інших пожежонебезпечних чинників), з метою своєчасного планування та

здійснення заходів щодо запобігання виникненню і ліквідування пожеж та їх наслідків (ДСТУ 7295:2013).

Моніторинг радіаційної безпеки це спостереження і контролювання рівня радіоактивного забруднення місцевості, повітря, води, продовольства, об'єктів господарювання, дозових навантажень на населення з метою прийняття оперативних рішень щодо запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг хімічної небезпеки це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо визначення ступеня і характеру хімічного забруднення довкілля, санітарногігієнічний нагляд за дотриманням установлених нормативів з метою виявлення джерела надходження небезпечних хімічних речовин, запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Збір та аналіз інформації про стан довкілля під час мирного та воєнного стану дає можливість приймати оперативні рішення для адекватного реагування на ситуацію.

4.3. Висновки до розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки в надзвичайних ситуаціях, висвітлено питання функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного час.

ВИСНОВКИ

При реалізації функції розпізнавання користувача за БО в ДС, необхідно враховувати ряд вимог. Одна з них - для отримання доступу в приміщення відвідувачеві не доводилося б виконувати ряд додаткових дій, відмінних від тих, які він виконує при доступі за допомогою набору коду або електронного ключа. Друге, необхідно враховувати вимогу до точності розпізнавання, незалежно від зовнішніх умов. Таким чином, відповідні БО для ДС – це геометрія обличчя і голос відвідувача. Методи, котрі базуються на цих ознаках, мають приблизно однакову точність.

В роботі отримані наступні результати:

– описано особливості контролю доступу в ДС. Набір коду доступу на ПВ, використання контактних або безконтактних ключів, в даний час є найбільш поширеним способом отримання доступу в приміщення;

– проаналізовано різні методи розпізнавання людини за БО;

– визначено, що метод розпізнавання, котрий базується на геометрії обличчя, має найкраще співвідношення точності і зручності та може бути використаний як основний для автоматичного розпізнавання користувача в ДС;

– здійснено порівняння існуючих на ринку аналогів ДС;

– проаналізовані основні методи розпізнавання за зображенням особи;

– описані задачі розпізнавання осіб на зображеннях і методи їх вирішення (детектування особи на зображенні, нормалізація зображення обличчя, обчислення ключових ознак і зіставлення з еталоном);

– наведено особливості методів підвищення точності алгоритмів розпізнавання зображення особи;

– докладно описано алгоритм ідентифікації користувача в ДС за зображенням особи. Запропонований алгоритм містить дві основні стадії: навчання та ідентифікація. На обох стадіях попередня обробка зображення особи і

обчислення його ключових ознак виконуються за ти самими алгоритмами з однаковими параметрами.

Беручи до уваги результати проведених експериментів можна зробити висновок, що програмний компонент реалізує запропонований алгоритм і може застосовуватися при розробці модулів ДС для контролю доступу в приміщення з невеликими базами зареєстрованих осіб, близько 15-20 осіб. Це можуть бути приватні будинки, невеликі офіси, службові приміщення тощо. Проведення додаткових досліджень, спрямованих на виявлення більш досконалих методів компенсації зміни освітленості в отриманих зображеннях осіб, а так само методів класифікації дозволить підвищити надійність алгоритму і застосовувати програмні рішення на його основі в більш широкій сфері, де для контролю доступу використовуються ДС.

Надалі робота може бути продовжена за рахунок комбінування методів. Наприклад, для зменшення ймовірності підробки, можна на додачу до розпізнавання за геометрією обличчя використати спосіб розпізнавання за рухами губ. Подібні роботи вже проводилися, так в статті [13] автори описують систему, в якій виконувалося розпізнавання одночасно за трьома ознаками: геометрії обличчя, руху губ і голосу. Такий підхід може істотно підвищити надійність системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Історія домофонії. URL: https://omo.systems/ua/istoriya-domofoni%D1%97/ (дата звертання: 06.11.2021).

2. Мослифт. Наша история. URL: http://www.moslift.ru/ (дата звертання: 06.11.2021).

3. Домофон. URL: https://ua.wikipedia.org/wiki/Домофон (дата звертання: 06.11.2021).

4. Контактна память. URL: https://ua.wikipedia.org/wiki/ Контактна_пам’ять (дата звертання: 07.11.2021).

5. RFID. URL: https://ru.wikipedia.org/wiki/RFID (дата звертання: 08.11.2021).

6. Биометрия. Международный фонд автоматической идентификации. URL: http://www.fond-ai.ru/art1/art228.html (дата звертання: 06.11.2021).

7. Кухарев, Г. А. Биометрические системы. Методы и средства идентификации личности человека. Монография. Санкт-Петербург: Политехника, 2001. 240 с.

8. Современные биометрические методы идентификации. Хабрахабр. URL: https://habrahabr.ru/post/126144/ (дата звертання: 07.11.2021).

9. Установление личности по голосу. Речевые технологии. URL: http://speetech.by/press/analytics/8 (дата звертання: 09.11.2021).

10. The Gira door communication system. URL: http://www.gira.com/en /tuerkommunikation.html (дата звертання: 12.11.2021).

11. Gira Keyless In Fingerprint. URL: http://www.gira.com/en/ gebaeudetechnik/produkte/keyless-in/fingerprint.html (дата звертання: 11.11.2021).

12. Fermax. URL: http://www.fermax.com (дата звертання: 12.11.2021).

13. Robert W.Frischholz, Ulrich Dieckmann BioID: A multimodal biometric identification system. *Computer* – March 2000. №33(2), pp. 64–68.

14. Татаренков Д. А. Анализ методов обнаружения лиц на изображении. *Молодой ученый*. 2015. №4. С. 270–276.

15. Viola P. and Jones M. J., «Rapid Object Detection using a Boosted Cascade of Simple Features». *IEEE Conf. on Computer Vision and Pat-tern Recognition (CVPR 2001)*. 2001. vol. 1. pp. 511–518.

16. Viola P. and Jones M. J., «Robust real-time face detection». *International Journal of Computer Vision*. 2004. vol. 57, no. 2. pp.137–154.

17. Turk M. and Pentland A. Face recognition using eigenfaces. Computer Vision and Pattern Recognition, 1991. Proceedings {CVPR'91.}, {IEEE} Computer Society Conference on 1991.

18. Belhumeur P N, and Hespanha J.P. and Kriegman. D. Eigenfaces vs. Fisher-faces: recognition using class specific linear projection, 1997.

19. Wiskott L., Fellous J.-M., Kuiger N., and von der Malsburg C., «Face recognition by elastic bunch graph matching». *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1997. vol. 19. pp. 775–779.

20. Шевчук Ю.В. Алгоритм ідентифікації відвідувача в домофонній системі за зображенням особи. Інформаційні моделі, системи та технології: Праці IX наук.-техн. конф. (Тернопіль, 08-09 грудня 2021 р.), Тернопіль, 2021. – С. 143.

21. Hieu V. Nguyen and Li Bai Cosine Similarity Metric Learning for Face Verification ACCV 2010.

22. Laura Sanchez Lopez. Local Binary Patterns applied to Face Detection and Recognition. Final Research Project. November 2010.

23. A decision-theoretic generalization of on-line learning and an application to boosting Journal of Computer and System Sciences, 1997. – no. 55.

24. Ahonen T., Hadid A., Pietikainen M. Face Recognition with Local Binary Patterns. *Lecture Notes in Computer Science*, 2004.

25. ГОСТ Р ИСО/МЭК 19795-1 – 2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы 71

испытаний в биометрии. Часть 1. Принципы и структура. Введ. 2008-12-25. М.: Стандартинформ, 2009. – 57 с.

26. Современные биометрические методы идентификации. URL: http://mx1.algoritm.org/arch/?id=37&a=916 (дата звертання: 19.11.2021).

27. Tan X. and Triggs B.. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *Lecture Notes in Computer Science*, 2007. vol. 4778. p. 168.

28. Krishna Dharavath, Fazal Ahmed Talukdar and Rabul Hussain Laskar. Improving Face Recognition Rate with Image Preprocessing. *Indian Journal of Science and Technology*, August 2014. vol. 7(8). pp. 1170–1175.

29. Ojala T, Pietikainen M, Maenpaa T. Multiresolution grayscale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2002. 24(7). pp. 971–87.

30. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. 2011. 215 с.

ДОДАТОК А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.932.72
Ю.В. Шевчук, Н.Б. Стадник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АЛГОРИТМ ІДЕНТИФІКАЦІЇ ВІДВІДУВАЧА В ДОМОФОННІЙ СИСТЕМІ ЗА ЗОБРАЖЕННЯМ ОСОБИ

UDC 004.932.72
Yu.V. Shevchuk, N.B. Stadnyk

VISITOR IDENTIFICATION ALGORITHM IN THE INTERCOM SYSTEM BY PERSONAL IMAGE

На точність результатів систем розпізнавання за зображенням особи в домофонних системах впливає ряд факторів, серед яких – неконтрольовані умови освітленості навколишнього середовища. Зображення, зняті при таких умовах, мають нерівномірний розподіл рівня сірого, що є причиною різної контрастності одержуваного зображення. Недостатнє освітлення і недосконалість обладнання - причина появи шумів. Все це необхідно враховувати при розробці алгоритмів розпізнання. Основні методи підвищення точності алгоритмів розпізнавання зображення особи - вирівнювання гістограми, гамма корекція, фільтр Гауса, медіанний фільтр.

Будь-який алгоритм ідентифікації осіб повинен вирішувати завдання локалізації особи на зображенні, його нормалізації, обчислення ключових ознак і класифікацію. Запропонований в роботі алгоритм розпізнавання осіб в ДС вирішує ці завдання, відміна від базового полягає в тому, що результатом роз'язання задачі локалізації обличчя є координати очей. Виділення обличчя за координатами очей, і його нормалізація виділені в окреме завдання попередньої обробки вхідного зображення.

Запропонований алгоритм містить дві основні стадії: навчання та ідентифікація. На обох стадіях попередня обробка зображення обличчя і обчислення його ключових ознак виконуються за ти самими алгоритмами з однаковими параметрами. Результатом навчання буде набір шаблонів, що описують класи (зареєстровані користувачі), результатом ідентифікації - приналежність вхідного зображення особи до певного класу шляхом порівняння вектора ознаки невідомої особи з вектором ознак осіб з навчальної вибірки.

Завдання попередньої обробки вхідного зображення спрямоване на виділення особи і її геометричне вирівнювання за координатам очей. Точки визначаються вручну на стадії навчання, і додаються у вигляді мета-інформації до зображення. На стадії ідентифікації виявлення особи використовується метод Віоли-Джонса. На етапі попередньої обробки з метою зменшення впливу фактора недостатньої або нерівномірної освітленості застосовується метод гама-корекції. Варто зазначити, що для домофонних систем отримання зображення обличчя відвідувача ведеться при неконтрольованих умовах освітленості, і компенсація впливу освітленості на зображенні завдання важлива, від вирішення її залежить точність розпізнавання.

Для обчислення вектора ознак для особи пропонується використовувати метод заснований на локальних бінарних шаблонах. Метод отримав найбільше поширення при вирішенні завдань пов'язаних з розпізнаванням осіб за рахунок своєї простоти, швидкості виконання і інваріантності до освітленості. Також метод має безліч модифікацій, спрямованих на підвищення його ефективності.

Основні кроки алгоритму: визначення ключових точок особи на зображенні; інтегральне представлення зображень; ознаки Хаара; бустінг; використання каскадів ознак; навчання класифікатора Віоли-Джонса; виділення та попередня обробка зображення обличчя; обчислення вектора ознак; навчання; ідентифікація.

ДОДАТОК Б

Перелік функцій програмних модулів

Головний модуль програми (program.cpp) :

Training – виконує навчання алгоритму;

Identification – виконує ідентифікацію осіб на відеофрагменті з тестової вибірки;

main – запускає основний потік програми.

Модуль бази даних (database.cpp):

database_initialize - ініціалізує контекст модуля;

database_get_predict_sessions - вибирає з директорії \ Database \ predict_set ідентифікатори транзакцій для розпізнавання осіб;

database_get_training_frames - вибирає з директорії \ database \

training_set зображення осіб тренувальної вибірки і повертає їх у масив;

database_create_framebuffer - формує для вказаної транзакції відеобуфер;

database_save_index - зберігає список ID осіб навчальної вибірки;

database_open_index - відкриває збережений список ID осіб навчальної вибірки;

database_save_histograms - зберігає обчислені гістограми (Вектора ознак) для будь-якої людини з навчальної вибірки;

database_open_histograms - відкриває збережені гістограми осіб навчальної вибірки;

database_write_predict_log - пише в журнал результати ідентифікації осіб.

Модуль детекції особи на зображенні (detection.cpp):

detection_initialize - ініціалізує контекст модуля;

detection_get_face - детектує обличчя на зображенні і нормалізує його.

Модуль ідентифікації особи (identification.cpp):

identification_initialize - ініціалізує контекст модуля;

identification_train - виконує навчання алгоритму за даними, отриманими за допомогою функції database_get_training_frames;

identification_extract_feature_vector - обчислює вектор ознак для заданого зображення особи;

identification_define_nearest_identity - для заданого вектора ознак визначає найбільш ймовірний ID користувача з навчальної вибірки;

identification_get_identity - з множини ID користувачів, отриманиих функцією identification_define_nearest_identity, вибирає найбільш ймовірного.