Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Модернізація автоматизованої системи ідентифікації особи на виробничому підприємстві шляхом розроблення комбінованого каскаду класифікаторів
(тема)

Виконав:
здобувач 2 року, групи КІТПВм-23-3
Нестеренко В. В.
(прізвище, ініціали)
Спеціальності 174 Автоматизація, комп`ютерно-інтегровані технології та робототехніка
(код і повна назва спеціальності)
Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Комп`ютерно-інтегровані технологічні процеси і виробництва
(повна назва освітньої програми)
Керівник доц. Аллахверанов Р. Ю.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри КІТАР _____ Невлюдов І. Ш.
(підпис) (прізвище, ініціали)

2025р.

Харківський національний університет радіоелектроніки

Факультет	Автоматики і комп'ютеризованих технологій
Кафедра	Комп'ютерно-інтегрованих технологій, автоматизації та роботехніки
Рівень вищої освіти	другий (магістерський)
Спеціальність	174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Тип програми	освітньо-професійна
Освітня програма	Комп`ютерно-інтегровані технологічні процеси і виробництва

(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри КІТАР _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Здобувачеві *Нестеренка Вячеславу Вячеславовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Модернізація автоматизованої системи ідентифікації особи на виробничому підприємстві шляхом розроблення комбінованого каскаду класифікаторів*
затверджена наказом по університету від " 22" *листопада* 2024*р*. №1231 Ст.
2. Термін подання здобувачем роботи " 22 " *січня* 2025*р.*
3. Вихідні дані до роботи 3.1 *Функція системи: контроль управління доступом до виробничого підприємства за результатами ідентифікації особи*;
3.2 *Бібліотека комп'ютерного зору – OpenCV*;
3.3 *Мова програмування* – C++;
3.4 *ОС – Microsoft Windows* 10;
3.4 *Оформлення текстової документації – ДСТУ* 3008-2015.

4. Перелік питань, що потрібно опрацювати в роботі 4.1 *Вступ*;
4.2 *Аналіз автоматизованих систем біометричної ідентифікації*;
4.3 *Структурне проєктування системи програмного контролю доступу на виробничє підприємство за технологією ідентифікації особи*;
4.4 *Розробка програмного контролю доступу на виробничє підприємство за технологією ідентифікації особи*;
4.5 *Охорона праці*;
4.6 *Висновки*.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Демонстраційний матеріал представлений у форматі PowerPoint* (**.ppt*) – 16 *с. формату* А4

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз автоматизованих систем біометричної ідентифікації*	25.11 – 30.11.24	*виконано*
2	*Структурне проєктування системи програмного контролю доступу на виробничє підприємство за технологією ідентифікації особи*	01.12 – 12.12.24	*виконано*
3	*Розробка програмного контролю доступу на виробничє підприємство за технологією ідентифікації особи*	13.12 – 31.12.24	*виконано*
4	*Охорона праці*	01.01 – 06.01.25	*виконано*
5	*Оформлення пояснювальної записки*	07.01 – 10.01.25	*виконано*
6	*Подання роботи на перевірку Інтернет-системою StrikePlagiarism*	11.01 – 13.01.25	*виконано*
7	*Подання роботи на рецензію*	14.01 – 17.01.25	*виконано*
8	*Подання роботи на підпис зав. кафедри*	18.01 – 21.01.25	*виконано*
9	*Подання кваліфікаційної роботи в ЕК*	22.01.25	*виконано*

Дата видачі завдання 25 *листопада* 2024 р.

Здобувач _____ *Нестеренко В. В.*
(підпис)

Керівник роботи _____ *доц. Аллахверанов Р. Ю.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 2 табл., 24 рис., 2 дод., 20 джерел.

БІОМЕТРИЧНІ СИСТЕМИ, ІДЕНТИФІКАЦІЯ, ВЕБКАМЕРА, ЗАХИСТ ІНФОРМАЦІЇ, КАСКАДИ, КОМП’ЮТЕРНИЙ ЗІР, СИСТЕМА, РОЗПІЗНАВАННЯ ОБРАЗІВ, СКАНУВАННЯ.

Мета роботи – розроблення програмного забезпечення для підвищення ефективності контроля доступа до виробничого підприємства, що ґрунтується на результатах ідентифікації особи із залученням системи комп'ютерного зору.

Об’єкт дослідження – ідентифікація особи за біометричними даними.

Предмет дослідження – метод сканування та розпізнавання образів у біометричних системах захисту інформації.

Методами дослідження було обрано методи декомпозиції систем, методи розпізнавання образів, методи створення систем комп’ютерного зору, інформаційні технології проєктування систем.

Розроблено програмне забезпечення ідентифікації за допомогою розпізнавання особи за геометрією обличчя, котре сприятиме захисту від несанкціонованого доступу на виробниче підприємство.

Окреслений програмний продукт може функціонувати в дуже широкому спектрі сфер діяльності людини, зокрема, з метою встановлення особи людини в реальному часі системами відеоспостереження, для пошуку та надання даних (системи безпеки) тощо.

ABSTRACT

Explanatory note: 72 pp., 2 tab., 24 figs., 2 appendices, 20 sources.

BIOMETRIC SYSTEMS, IDENTIFICATION, WEBCAM, INFORMATION PROTECTION, CASCADES, COMPUTER VISION, SYSTEM, PATTERN RECOGNITION, SCANNING.

The goal of the work is to develop software to enhance the efficiency of access control at a production enterprise, based on the results of personal identification using a computer vision system.Object of research – biometric information security systems.

The object of the research is personal identification based on biometric data.

The research methods were chosen: methods of system decomposition, methods of pattern recognition, methods of creating computer vision systems, information technology for system design.

The software for identification by facial geometry recognition has been developed, which will help protect against unauthorized access to a manufacturing enterprise.

This software product can function in a very wide range of human activities, in particular, to establish a person's identity in real time by video surveillance systems, to search and provide data (security systems), etc.

Я, як студент ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

«20» січня 2025 р. _____ Нестеренко В. В.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БД – база даних;

БСКД – біометричні системи контролю доступу;

ДНК – дезоксирибонуклеїнова кислота;

КПО – коефіцієнт природної освітленості;

ПЕОМ – персональна електронно-обчислювальна машина;

ПК – персональний комп’ютер;

ПЗ – програмне забезпечення;

СЗІ – системи захисту інформації;

ТОВ – товариство з обмеженою відповідальністю;

AAM – Active Appearance Model;

APFIS – Automated Palmprint and Fingerprint Identification Biometric System;

DFD – Data Flow Diagrams;

FAR – False Accept Rate;

FRR – False Reject Rate;

IDE – Integrated Development Environment;

IDEF – Integration Definition for Function Modeling;

PCA – Principal component analysis;

SURF – Speeded-Up Robust Features.

ВСТУП

На сьогодні проблема ідентифікації особи вважається вкрай актуальною і важливою для досягнення різноманітних цілей, зокрема, здійснення контролю під час перетину кордону, отримання особою доступу до приміщень з обмеженим доступом, а також доступу до конфіденційної інформації.

Розпізнавання облич користується попитом та визнанням завдяки своїм значним перевагам. Однак водночас дана технологія може спричинити стурбованість і тривогу. Отже, доцільність встановлення правильного балансу між перевагами та недоліками стає важливою темою як для виробників систем безпеки, так і для користувачів.

Поширений сьогодні біометричний метод ідентифікації, наприклад, впізнавання особи за відбитками пальців або сітківкою ока, голосом тощо також є досить надійним у порівнянні з магнітними картками. Проте ідентифікація особи за обличчям є більш зручною для використання, оскільки працює швидше та не потребує фізичного контакту зі зчитувачем, що наразі є дуже нагальним. Отже, тема кваліфікаційної роботи магістра - актуальна.

Мета роботи полягає у розробленні програмного забезпечення для підвищення ефективності контроля доступа до виробничого підприємства, що ґрунтується на результатах ідентифікації особи із залученням системи комп'ютерного зору.

Об’єктом дослідження є ідентифікація особи за біометричними даними.

Предметом дослідження є метод сканування і розпізнавання образів у біометричних системах захисту інформації.

Методами дослідження було обрано методи декомпозиції систем, методи розпізнавання образів, методи створення систем комп’ютерного зору, інформаційні технології проєктування систем.

Для досягнення поставленої мети необхідно розв’язати наступні завдання:

– вивчити основні поняття біометричних технологій і систем захисту інформації;

– проаналізувати наявні методи розпізнавання обличчя, а також принципи їхньої роботи;

– реалізувати програмний метод ідентифікації обличчя людини і дослідити результати його роботи;

– визначати небезпечні та шкідливі виробничі чинники в лабораторії, в якій виконувалися дослідження;

– розробити заходи та технічні засоби щодо забезпечення безпеки праці працюючого персоналу лабораторії.

Работа виконується згідно з [1-4], як складова наукових досліджень, які здійснюються на кафедрі КІТАР Харківського національного університету радіоелектроніки, результати дослідження опубліковані у [5, 6].

1 АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Термін «біометрія» походить від слів «bio» (життя) і «metron» (міра) та позначає як науку, так і технологію вимірювання, а також статистичне обчислення біологічних даних. У загальному випадку біометрія визначається як сукупність автоматизованих методів ідентифікації та/або аутентифікації людей на основі їхніх фізіологічних характеристик, зокрема, відбитків пальців, геометрії долоні, сітківки чи райдужної оболонки очей, зразків голосу, а також геометрії особи.

Біометрикою називають наукову дисципліну, що вивчає способи вимірювання різних параметрів людини з метою встановлення подібності або відмінностей між людьми і виокремлення однієї конкретної людини з безлічі інших людей. Таким чином, це наука, котра вивчає методики розпізнавання конкретної людини за її індивідуальними параметрами.

За біометричні характеристики прийнято брати вимірні фізіологічні риси людини, що можна використовувати для встановлення особи або перевірки декларованих особистих даних.

Біометричними технологіями вважаються автоматичні чи автоматизовані методи розпізнавання особи людини за її біологічними характеристикам [5].

Будь-яка біометрична система устаткована біометричним сканером, тобто фізичним пристроєм, який дозволяє зчитувати ту або іншу біометричну характеристику, а також містить алгоритм порівняння вимірюваної характеристики з попередньо зареєстрованою (біометричним шаблоном).

Біометричною ідентифікацією називають автоматизований метод розпізнавання особистості, котрий ґрунтується на базі унікальних фізіологічних характеристик.

Загальні принципи роботи біометричних технологій полягають у реалізації наступних етапів:

– реєстрації ідентифікатора, де відомості про фізіологічні характеристики перетворюються на форму, доступну комп'ютерним технологіям, і вносяться в пам'ять біометричної системи. Вебкамера або інші датчики сканують людину, щоб створити її цифрове відтворення. Власне сканування обличчя в середньому триває 20 – 30 с, у результаті чого формуються кілька зображень [6]. В ідеальному випадку такі зображення фіксуватимуть злегка різні ракурси та вирази обличчя, що дозволить отримати більш точні дані;

– виділенні, тобто етапі, в якому з пред'явленого ідентифікатора визначаються унікальні ознаки, аналізовані системою. Спеціальний програмний модуль обробляє дане зображення та визначає характерні особливості особи, а потім створює шаблон. Існують деякі частини обличчя, котрі з плином часу практично не змінюються, як-от: верхні обриси очниць, області зовнішньої вилиці та край рота. Більшість алгоритмів, які було розроблено для біометричних технологій, дозволяють враховувати можливі зміни в зачісці людини, через те, що вони не використовують для аналізу ділянки обличчя вище межі росту волосся. Шаблон зображення особи, котру було відтворено, зберігається в базі даних (БД) біометричної системи;

– зіставленні відомостей під час порівняння про пред'явленого знову та раніше зареєстрованого ідентифікатора. Отримані дані порівнюються зі збереженим у БД шаблоном з метою визначення, чи відповідають ці зображення одне одному. Ступінь подібності, необхідний для перевірки, є порогом, який може бути відрегульований відповідно до різного типу персоналу в залежності від прав доступу, потужності ПЕОМ, часу доби й низки інших чинників;

– рішенні, що полягає у висновку про те, чи збігаються або не збігаються ідентифікатори пред'явлений знову та зареєстрований раніше. Висновок про збіг або розбіжності ідентифікаторів також може транслюватися іншим системам, наприклад, системам контролю і керування доступом, системам захисту інформації тощо, котрі приймають рішення з урахуванням отриманої інформації.

Порівняння біометричних ідентифікаторів може реалізовуватись у двох режимах: ідентифікації і аутентифікації.

Під час ідентифікації порівняння виконується в режимі «один-до багатьох»: пред'явлений знову ідентифікатор порівнюється з усіма, зареєстрованими раніше. До того ж біометрична система аналізує весь перелік ідентифікаторів, відомості про яких були зареєстровані раніше.

Під час аутентифікації співставляються відомості про двох конкретних ідентифікаторів. За приклад візьмемо порівняння відомостей про пред'явленого знову ідентифікатора з відомостями, записаними до пам'яті спеціальної карти. Зважаючи на це, необхідно пред'являти як біометричний ідентифікатор, так і карту.

Системи, котрі функціонують у режимі аутентифікації, здебільшого, є повністю автоматичними (рішення приймають без участі людини).

З метою прискорення розпізнавання користувачеві може бути запропоновано використання додаткового ідентифікатора, на кшталт PIN-коду, котрий позначає номер відділу, секції тощо. У даному разі в режимі ідентифікації виконується порівняння не з усім списком, а тільки з його частиною, що виділяється зважаючи на введене додатковим ідентифікатором.

Схему роботи біометричних систем продемонстровано на рисунку 1.1.

У біометричних системах можуть виникати помилки. У зв’язку з цим контрольний шаблон може бути визнаний як відповідний еталонному шаблон іншої особи (помилка типу I, ймовірність помилкового допуску, FAR – False Accept Rate) або як невідповідний еталонному шаблон даного користувача, незважаючи те, що даний конкретний користувач зареєстрований у біометричній системі (помилка типу II, ймовірність помилкової відмови в доступі, FRR – False Reject Rate).

Рисунок 1.1 – Схема роботи біометричних систем

Діапазон проблем, розв’язання яких може полягати у застосуванні біометричних технологій, містить [7-9]:

– запобігання проникненню зловмисників на території та приміщення, що охороняються, шляхом підроблення, крадіжки документів, карт, паролів;

– обмеження доступу до інформації, а також забезпечення персональної відповідальності за її збереження;

– забезпечення допуску до відповідних об'єктів тільки сертифікованих фахівців;

– можливість уникнути накладних витрат, які пов'язані з експлуатацією системи контролю та керуванням доступом (карти, ключі);

– виключення незручностей, які пов'язані з втратою, псуванням або забування ключів, карт, паролів;

– організацію обліку доступу та відвідування співробітниками.

Біометричні системи безпеки розв’язують такі завдання:

– істотно знижують імовірність проникнення небажаної особи до зони з обмеженим доступом;

– створюють психологічний бар'єр для потенційного зловмисника;

– підтверджують документально факт певної дії кожною людиною.

1.2 Аналіз видів біометричних систем захисту інформації

Системи ідентифікації, котрі аналізують характерні риси людини, можна розподілити на дві великі групи: фізіологічні (статичні характеристики) та поведінкові чи психологічні (динамічні характеристики).

Статичні методи ідентифікації ґрунтуються на аналізі незмінних фізіологічних характеристик людини, зокрема:

– відбитках пальців (на опрацюванні даних ідентифікаторів будується найпоширеніша і зручна біометрична технологія);

– формі та геометрії обличчя;

– формі та будові черепа;

– сітківці ока (фактично не використовується як ідентифікатор);

– райдужної оболонки ока;

– геометрії долоні, кисті руки або пальця (застосовується у вузькому сегменті ринку);

– термографії обличчя, термографії руки (технології, засновані на використанні цих ідентифікаторів, не набули поширення);

– малюнках вен на долоні або пальці руки;

– ДНК (використовується в галузі спеціалізованих експертиз).

Динамічні методи ідентифікації базуються на аналізі поведінкових характеристик особистості, тобто особливостей, які властиві кожній людині в процесі відтворення якоїсь дії. У свою чергу, динамічні методи істотно поступаються статичним у точності й ефективності і, зазвичай, використовуються як допоміжні. Ідентифікаторами можуть бути динаміка підпису чи клавіатурного набору, особливості накреслення рукописного тексту, голос, а також рух губ, хода.

Фізіологічні системи вважаються більш надійними, оскільки вони ґрунтуються на індивідуальних особливостях людини, що практично не

змінюються під впливом її психоемоційного стану. Поведінкові методи оцінюють дії індивідуума, надаючи при цьому користувачу певний рівень контролю над його вчинками. Біометрія, котра базується на цих методах, враховує високий ступінь внутрішньоособистісних варіацій. Зважаючи на те, що настрій або стан здоров'я впливають на оцінювану характеристику, відповідно поведінкові методи найкраще працюють за умови регулярного використання пристрою. Поведінкові характеристики, зокрема, підпис, клавіатурний почерк, хода або голос перебувають під впливом керованих дій і менш керованих психологічних чинники. З огляду на те, що поведінкові характеристики з плином часу можуть змінюватися, зареєстрований біометричний зразок повинен оновлюватися під час кожного його застосування. Незважаючи на те, що біометрія, котра ґрунтується на поведінкових характеристиках, менш вартісна, проте фізіологічні риси сприяють проведенню процесу ідентифікації особи з більш високою точністю.

Разом з тим біометричні системи ідентифікації особи розрізняються також за низкою інших показників. Серед них можна виділити такі:

– пропускну здатність;

– вартість;

– надійність з позиції ідентифікації;

– простоту та зручність під час використання;

– ступінь психологічного комфорту користувача;

– спосіб зчитування;

– точність обчислення автентичності;

– збільшену продуктивність;

– витрати на обслуговування;

– можливість інтеграції;

– конфіденційність.

Пропускна здатність системи характеризується часом, протягом якого обслуговується один користувач. Крім того, вона залежить від режиму роботи пристрою – процесу ідентифікації чи аутентифікації. Під час проведення

ідентифікації користувача витрачається більше часу, ніж для режиму аутентифікації, оскільки зі зразком необхідно порівняти майже всі шаблони, занесені до БД. У режимі аутентифікації системі достатньо порівняти пропонований зразок із одним шаблоном.

Вартість - це один із визначальних чинників широкого використання біометричних систем. Вона є досить високою в країнах-виробниках і значно зростає, коли такі системи доходять до кінцевих споживачів. Проте вітчизняні розробки є набагато дешевшими, незважаючи на те, що їхня якість не поступається системам західних аналогів.

Аспект надійності біометричної системи доцільно розглядати з позиції ідентифікації. Проте можливі й два види помилок: «помилкові відмови» (система не визнала «свого»), а також «неправдиві допуски» (система прийняла «чужого» за «свого») [8]. Отже, чим менше система пропускає «чужих» і відкидає законних користувачів, тим дана система є надійнішою.

Простоту та зручність у функціонуванні багато в чому визначають споживчі властивості біометричних систем. З огляду на це, критеріями оцінки системи виступають такі показники, зокрема, легкість інсталяції даної біометричної системи, а також швидкість отримання характеристик (без активної участі користувача), до того ж, час, який необхідний для навчання роботі з системою.

За ступенем психологічного комфорту визначають, наскільки ті чи інші системи і методи розпізнавання біометричних характеристик здатні викликати у користувачів негативну реакцію, страх або сумнів. Наприклад, деякі люди лякаються дактилоскопії, а інші – не бажають дивитися у відеокамеру.

За способом зчитування розрізняють біометричні системи дистанційні та контактні.

Продуктивність системи залежить від таких властивостей, як точність, вартість, інтеграція, а також зручність у використанні.

Фізіологічні розпізнавальні методи подано в таблиці 1.1 [10].

Аналіз наведеної таблиці дозволяє зробити такі висновки:

– універсального ідентифікатора, котрий підходить для всіх сфер діяльності і рівнів захисту певного об'єкта, не існує;

– під час вибору конкретної біометричної технології доцільно враховувати переваги і недоліки ідентифікатора, котрий використовують, а також характеристики об'єкта, що охороняється;

– необхідно передбачати перспективи застосування біометричного ідентифікатора також для розв’язання інших завдань, крім контролю фізичного доступу.

Таблиця 1.1 – Порівняльний аналіз можливостей застосування технологій біометричної ідентифікації в системі контролю і керування доступом

Ідентифікатор	Переваги	Недоліки
1	2	3
Відбиток Пальця	Зручність, надійність (у зв'язку з тривалим застосуванням даного методу), незмінність ідентифікатора у дорослих людей, дешевизна обладнання та програмного забезпечення (ПЗ), велика кількість ідентифікаторів (десять пальців рук проти двох очей, одного обличчя тощо).	Наявність невеликої кількості людей, відбитки пальців яких розпізнаються погано, контакт зі сканером відбитків, вплив температурних і фізіологічних чинників (складність розпізнавання пальців, які побували в умовах низьких температур)
Геометрія обличчя (2D-технології)	Відсутність необхідності контактувати зі сканувальним пристроєм, можливість застосування в місцях масового скупчення людей (аеропорти, вокзали тощо), максимальна соціальна прийнятність.	Найнижчий відсоток успішного розпізнавання, велика чутливість до змін ідентифікатора (поява окуляр, бороди) і зовнішнім чинником (поворот голови, освітленість).
Геометрія руки	Надійність порівнянна з ідентифікацією за відбитками пальців	Дорожнеча і громіздкість сканерів, незручність процедури ідентифікації

Продовження таблиці 2.1

1	2	3
Будова черепа (3D-технології)	Відсутність необхідності контактувати зі сканувальним пристроєм.	Дорожнеча, громіздкість обладнання, низька швидкість ідентифікації, відсутність можливості обслуговувати велику кількість користувачів
Райдужна оболонка ока	Відсутність необхідності контактувати зі скануючим пристроєм, високий відсоток успішного розпізнавання	Мінливість ідентифікатора під впливом віку і стану нервової системи, чутливість до зовнішніх факторів (освітленість, колір шкіри), дорожнеча сканерів
Малюнок вен на долоні або пальці	Відсутність необхідності контактувати зі скануючим пристроєм, незмінність ідентифікатора протягом усього життя, низька чутливість сканерів до зовнішніх умов (температура навколишнього середовища, освітленість та ін.)	Необхідність точного розташування ідентифікатора по відношенню до сканера (на певній відстані), висока вартість сканерів, відсутність практики застосування технології при обслуговуванні великої кількості користувачів в режимі ідентифікації

1.3 Огляд існуючих рішень

1.3.1 Сканування райдужної оболонки

Метод біометричної ідентифікації особистості засновано на унікальних характерних ознаках райдужної оболонки ока. Райдужна оболонка є частиною ока й визначається як кольоровий круг, який обрамляє зіницю.

Процес сканування райдужної оболонки розпочинається з фотографії. У спеціальному фотоапараті, котрий, як правило, розташовують на відстань до

людини не ближче ніж на 90 см, вбудовано інфрачервоне підсвічування для отримання фото з дуже високою роздільною здатністю. Власне процес фотографування триває 1 – 2 с. Отримане детальне зображення райдужної оболонки перетворюється на схематичну форму, після чого записується і зберігається для подальшого порівняння.

Зображення райдужки є надзвичайно складним, оскільки містить у собі великий обсяг інформації, бо має понад 200 унікальних точок.

Технологія сканування райдужної оболонки - це один із найбільш надійних засобів ідентифікації. Така процедура не схильна до помилкового порівняння та фальсифікації, оскільки праве і ліве око людини відрізняються одне від одного, а їхні малюнки дуже легко зафіксувати в схематичній формі.

Частота помилкового розпізнавання в системах ідентифікації за райдужкою дорівнює від 1 млн. до 1,2 млн., статистично це набагато вище, ніж результати, продемонстровані в середньому системами розпізнавання за відбитками пальців [10].

Таким чином, метод ідентифікації за райдужною оболонкою забезпечує високий рівень безпеки користувача разом із захистом приватної інформації.

Розглянемо переваги та недоліки методу ідентифікації за райдужною оболонкою ока на прикладі застосування сканера Panasonic Authenticam BM-ET100US, продемонстрованого на рисунку 1.2.

Рисунок 1.2 – Сканер Panasonic Authenticam BM–ET100US

Перевагами методу сканування райдужної оболонки ока є:

– високий ступінь розпізнавання і, відповідно, незначна кількість помилок. Реєстрація лівого ока замість правого успіху не виявила. Результати досліджень патентовласника технології ідентифікації за райдужною оболонкою ока – компанії Iridian Technologies – показали, що у надзвичайно великій базі реєстрацій (983 млн.) ймовірність помилкового розпізнавання людини була нижчою за 0,000001, а ймовірність помилкової відмови в розпізнаванні - нижчою за 0,003;

– безконтактний спосіб сканування (на відстані від 1 м до 1,5 м) [10];

– малий обсяг БД;

– розпізнавання за фотографією з цифрової камери виявилося неможливим, отже, перспектива фальсифікації відхиляється [11];

– відсутність впливу зовнішніх чинників. Пряме сонячне освітлення чи його відсутність не відіграють ролі під час порівняння райдужних оболонок. Окуляри та контактні лінзи ніяк не впливають на якість зображення;

– система однаково успішно працює навіть у тому разі, коли у людини порушений зір, однак не пошкоджена райдужна оболонка [12].

Недоліками даного методу позначимо:

– дискомфорт. Користувач може відчувати незручність під час застосування даної системи;

– неприйнятність методу деякими людьми через певні хвороби. Крім того, впливати на результат можуть як вікові зміни райдужки, так і стан нервової системи;

– висока вартість ПЗ.

1.3.2 Голосова ідентифікація

Одним із видів біометричної ідентифікації, що привертає значний інтерес розробників і фахівців, є метод ідентифікації особи за голосом.

Голос і мова людини містять у собі безсумнівно індивідуальну інформацію. Власне тому вони і привертають увагу тих, хто зацікавлений у

використанні голосової біометричної інформації для різних застосунків. Особливість таких систем полягає в тому, що вони допускають віддалену аутентифікацію, наприклад, телефоном, що виключається іншими біометричними ідентифікаціями. Зручність для користувача пояснюється простотою, здатністю легко інтегруватися з іншими методами. Такі чинники є важливими та підтверджують доцільність застосування мовних технологій у біометричних системах як окремо, так і в комплексі з іншими методами аутентифікації й ідентифікації особи.

На сьогодні вже створено десятки різних систем ідентифікації за голосом, мають різні параметри і вимоги до процесу ідентифікації з урахуванням конкретних завдань. У нашій країні розроблено низку програмних продуктів, які вже знайшли застосування на практиці. Проте розроблені програми не відрізняються простотою навчання, зручністю роботи чи низькою вартістю. Здебільшого вони функціонують як додаткові засоби для перевірки достовірності там, де необхідно забезпечити високий ступінь надійності систем ідентифікації. Вдосконалення алгоритмів ідентифікації за мовним сигналом спрямовано на розв’язання таких питань, як створення імітостойкості алгоритму мовної ідентифікації. Крім того, розробників цікавить питання, котре пов'язано з віковими змінами голосу, а також пошук нових найбільш інформативних ознак для опису його індивідуальних особливостей.

На сьогодні було розроблено проєкт технічних вимог для створення системи контролю та керування доступом на базі мовної ідентифікації з метою доступу до фізичних об'єктів і інформаційних ресурсів. Система голосової текстозалежної аутентифікації, котра розрахована на багато користувачів, призначена для розмежування доступу користувачів до інформаційних ресурсів за спіральною фразою. Запропонована система повинна задовольняти необхідним вимогам з безпеки, мінімізуючи при цьому незручності для користувачів, які неминуче можуть виникати. У складі системи повинні бути елементи для створення та надсилання звукової інформації, а також засоби

керування виконавчими пристроями системи контролю та керування доступом. Така система повинна забезпечувати:

– розпізнавання особи користувача без безпосереднього контакту з ним;

– застосування мікрофонів широкого функціонування як технічних засобів введення для аутентифікації;

– ефективне розпізнавання живого голосу, виключаючи можливість використання записів з метою несанкціонованого доступу.

Проєктована система повинна характеризуватися такими можливостями:

– тонким налаштуванням системи для досягнення оптимального співвідношення безпеки і зручності використання для кожного конкретного користувача;

– розмежуванням прав доступу користувачів до ресурсів через систему пріоритетів;

– зручним і швидким додаванням нових користувачів до системи (без переривання роботи системи);

– цілодобовим безперервним режимом роботи системи;

– веденням журналу активності користувачів;

– віддаленим доступом для адміністрування системи та аудиту користувачів;

– автоматичним застосуванням декількох дисків для зберігання біометричних даних і журналів аутентифікації користувачів.

Процес оброблення ідентифікаторів у даній технології відбувається наступним чином. Мова людини розбивається на звукові сегменти, котрі потім перетворюються на цифрову модель. Під час подальшої ідентифікації порівнюються раніше зареєстрований і знову сформований «голосові відбитки».

Доцільно перелічити такі можливості і переваги мовних технологій ідентифікації:

– звичний для людини спосіб ідентифікації;

– низька вартість апаратних засобів у разі реалізації в складі комплексних систем безпеки (найнижча серед усіх біометричних методів);

– безконтактність;

– можливість віддаленої ідентифікації чи аутентифікації;

– неможливість для зловмисника імітувати голос за допомогою магнітофона, оскільки під час відтворення записаної мови через мініатюрні гучномовці до сигналу додаються спотворення, котрі перешкоджають ідентифікації мовця;

– можливість визначення під час ідентифікації людини, чи знаходиться вона під загрозою насильства, оскільки емоційний стан мовця спричиняє істотний вплив на характеристики голосу та мовлення;

– можливість підвищення надійності аутентифікації шляхом одночасного використання технологій ідентифікації за голосом і розпізнавання мови (сказаного пароля).

До недоліків даної технології можна віднести такі ознаки:

– складність процедури навчання систем (реєстрації користувачів);

– дороговартісне ПЗ;

– високий рівень помилок;

– потреба у спеціальному шумоізольованому приміщенні для проходження ідентифікації;

– можливість перехоплення фрази за допомогою звукозаписних пристроїв;

– залежність якості розпізнавання від багатьох чинників, зокрема, інтонації, швидкості мовлення, психологічного стану, хвороби горла тощо;

– необхідність підбору спеціальних фраз з метою підвищення точності розпізнавання;

– вікові голосові зміни, котрі призводять до необхідності періодично оновлювати збережений у системі еталон мови;

– надійність роботи системи залежить від якості каналу передавання мовного сигналу до системи ідентифікації. Наприклад, від таких його

характеристик: частотного діапазону, рівня нелінійних спотворень, відношення сигнал/шум тощо.

Найвища надійність роботи забезпечується в тому разі, коли еталон голосу клієнта і його запит надходять одним і тим же каналом, зокрема, телефонним. Отже, наразі системи мовної ідентифікації в системах контролю та керування доступом застосовуються як додаткові засоби перевірки достовірності спільно з іншими технологіями ідентифікації.

1.3.3 Дактилоскопічний метод біометрії

Ідентифікація за відбитками пальців вважається одією з найбільш поширених і ефективних біометричних технологій. Завдяки універсальності даної технології її можна використовувати практично у будь-якій сфері, а також для розв’язання будь-якої задачі, де необхідна достовірна ідентифікація користувачів.

Відбитки всіх пальців кожної людини є унікальними завдяки малюнкам папілярних ліній, відповідно, розрізняються навіть у близнюків. Відбитки пальців не змінюються протягом усього життя дорослої людини. Крім того, вони легко і просто зчитуються під час ідентифікації. Якщо один із пальців пошкоджений, то для ідентифікації можна скористатися «резервними», відомості про які також, як правило, вносяться до біометричної системи під час реєстрації користувача.

Для отримання інформації про відбитки пальців послуговуються спеціалізованими сканерами. Відбиток, який отримано за допомогою спеціалізованого сканера чи датчика, перетворюється на цифровий код і порівнюється з раніше введеним еталоном. Процес ідентифікації триває лічені секунди. Власне пристрій займає мало місця. Спосіб отримання відбитка продемонстровано на рисунку 1.3 [8].

Розрізняють три основних типи сканерів відбитків пальців:

– ємнісні;

– прокатні;

– оптичні.

Рисунок 1.3 – Сканування відбитка на терміналі
TouchPrint 3100 Live Scan

Ємнісні сканери вважаються найбільш дешевими, проте вони не відрізняються ні практичністю, ні довговічністю. Такі пристрої виходять з ладу відразу ж після того, як людина, чиї руки були наелектризовані, наприклад, через носіння одягу з вовняної або шовкової тканини, їх торкнулася. До того ж, дані сканери створюють зображення відбитків низької якості.

Найбільш досконала технологія ідентифікації за відбитками пальців втілюється через оптичні сканери. Вони є трохи дорожчими за сканери інших типів, однак характеризуються більшою довговічністю, економічністю та простотою у використанні. Зображення відбитків вирізняються високою якістю.

Прокатні сканери займають середню нішу. Зображення відбитка у таких сканерів формується шляхом «прокочування» відбитка через вузьке віконце сканера, після чого цілісне зображення ідентифікатора «зшивається» з окремих кадрів, отриманих під час проведення зазначеної процедури. У зв’язку з цим від користувача даного пристрою потрібно постійно дотримуватись однаковості в швидкості і манері «прокатування» відбитків, що досить складно.

Крім того, важливо, що дактилоскопічна експертиза обумовлена законодавчою юридичною базою, тому її результати можуть бути використані як аргументи в суді [11].

Лідером на ринку дактилоскопічної ідентифікації стала компанія «Sagem Défense Sécurité» (Франція), котра спеціалізується на виробництві обладнання для БСКД. Згідно з маркетинговим дослідженням, проведеним агентством «International Biometric Group» у 2015 році, частка продукції компанії на світовому ринку систем біометричної ідентифікації склала 80%.

З дня створення Sagem її системи біометричної ідентифікації зареєстрували понад 1 мільярд відбитків пальців, що дорівнює майже 1/6 населення земної кулі [11]. Компанія інвестує значні кошти в наукові дослідження, постійно вдосконалює технології біометричної ідентифікації й аутентифікації.

Нова концепція компанії APFIS (Automated Palmprint and Fingerprint Identification Biometric System) втілена до біометричних системм контролю доступу нового покоління Metamorpho, дозволяє проводити ідентифікацію за кількома ознаками: за відбитками пальців та/або долоні. До того ж, доповнена розпізнаванням іншого ідентифікатора.

Компанія Trans-Ameritech забезпечує європейський ринок простою та дешевою (всього 600 – 700 $) дактилоскопічною системою SACcat фірми SAC Technologies, яка контролює доступ до робочих станцій і серверів Windows, а також до відповідних ресурсів, котрі захищаються системою Windows. Водночас у системного адміністратора залишається можливість використовувати свій звичайний пароль, зареєстрований у Windows. Система спроможна забезпечити ефективний захист від несанкціонованого доступу для мереж фінансових організацій, медичних установ, страхових компаній, різних комерційних структур, індивідуальних робочих станцій тощо. Основна особливість даної системи контролю та керування доступом полягає у високій надійності у поєднанні із порівняно низькою вартістю.

До того ж, широкого поширення набув дактилоскопічний зчитувач FingerScan V20 UA швейцарської компанії Identix. Алгоритми ідентифікації BioEngineing і ID Safe, запатентовані в Identix, поєднанні з унікальністю біометричних параметрів пальця кожної людини забезпечують високий рівень надійності ідентифікації. FingerScan V20 користується популярністю серед засобів для контролю доступу до комп'ютерних систем. Зокрема один зчитувач FingerScan може зберігати в своїй пам'яті до 512 шаблонів відбитків пальців співробітників, яким дозволено доступ до мережі. Для великих систем контролю та керування доступом кількість шаблонів, які зберігаються на одному зчитувачі, може бути збільшено до 5000 або 32000 одиниць. Вірогідність несанкціонованого доступу до зчитувача відбитка пальця FingerScan V20 становить 0,0001 %. До того ж у даній моделі реалізована функція регулювання порога чутливості, що дає можливість гнучко налаштовувати систему з огляду на конкретні вимоги безпеки. Незважаючи на складність реалізованих алгоритмів ідентифікації, FingerScan V20 характеризується простотою в налаштуванні й експлуатації. Достатньо набрати код на клавіатурі, прикласти палець до сканувальної поверхні, і протягом 1 секунди зчитувач порівняє відсканований відбиток із занесеними до його пам'яті відбитками пальців співробітників. Зауважимо, що допустимий кут повороту пальця на біометричний зчитувач щодо еталонного становить ±18°. У зчитувачі FingerScan V20 реалізовано технологію біометричного контролю доступу ID Safe. На її основі можна побудувати систему контролю та керування доступом масштабу підприємства, котра забезпечить авторизованим особам доступ до комп'ютерних мереж.

Відомими є й багато інших компаній, які займаються технологіями контролю доступу з використанням відбитка пальця, як-от: T-NETIX, American Biometric Company, Attel Communication Ltd, Strartek тощо.

В Україні технологія дактилоскопічної ідентифікації представлена ТОВ «Технотрейд». Як приклад її розробок можна навести такий продукт – антивандальний зчитувач відбитків пальців SF101. Він спроєктований як

біометричний зчитувач, який розроблений для системи контролю та керування доступом. Крім того, найбільшою його перевагою є інтеграція з більшістю контролерів доступу, що існують на ринку. Вартість даного зчитувача близько 300 $.

1.3.4 Геометрія руки

У даному біометричному методі для ідентифікації особи використовується геометрична форма руки. Зважаючи на те, що людські руки не є чимось унікальним, вочевидь необхідно поєднувати кілька специфічних характеристик з метою забезпечення динамічної аутентифікації. Деякі пристрої для сканування вимірюють тільки два пальця, інші – повністю всю руку. Вимірювані характеристики ґрунтуються на:

– вигинах пальців, товщині та довжині;

– товщині та ширині тильної сторони руки;

– відстані між суглобами;

– загальній структурі кістки.

Зауважимо, що такі дії, як розпухання тканин або удари можуть спотворити вихідну структуру руки. Це може сприяти виконанню помилкового порівняння, проте кількість прийнятних збігів, які відрізняються, може бути відрегульовано відповідно до потреб певного рівня забезпечення безпеки.

На етапі реєстрації до системи сканування рука поміщається на рівну поверхню, передбачену для зчитування. Позиція руки фіксується за допомогою п'яти штифтів, які допомогають правильно розташувати руку відповідно до фотокамер. Послідовність фотокамер створює тривимірні зображення бічних сторін і тильної сторони руки. Сканування руки – це простий і швидкий процес, оскільки пристрій сканування може обробити тривимірні зображення за п'ять секунд, а аутентифікація займає не більше однієї секунди.

Надійність такої ідентифікації порівнюється з надійністю дактилоскопічної системи, хоча власне пристрій займає більше місця.

Більше десяти років успішно функціонує метод тривимірної ідентифікації HandKey, розроблений компанією Recognition Systems. Біометричний зчитувач HandKey II призначений для обмеження доступу до комп'ютерів і особливо до об'єктів, які знаходяться під охороною. З метою захисту від несанкціонованого розкриття корпусу зчитувач устаткований датчиком розтину.

Процедура ідентифікації особи за допомогою біометричного зчитувача HandKey II розподілена на два етапи. Спочатку на клавіатурі співробітник набирає свій унікальний ідентифікаційний номер з 1 – 10 цифр, а потім зчитувач сканує кисті руки і порівнює отриману інформацію з еталонною. До того ж, замість набору PIN-коду в HandKey II передбачено під’єднання зчитувача електронних карт доступу. Двоетапна процедура ідентифікації користувача істотно підвищує рівень безпеки.

1.3.5 Геометрія обличчя

Ідентифікація за обличчям стає досить поширеною технологією, проте застосовується як допоміжна по відношенню до інших біометричних методів, наприклад, ідентифікації за відбитками пальців, або іншим способам встановлення особи людини.

Функціонують різні системи ідентифікації за обличчям. Деякі з них будують цифровий образ обличчя людини, ґрунтуючись на двовимірних зображеннях, інші використовують тривимірні. Під час ідентифікації біометрична система автоматично виділяє й опрацьовує відомості, котрі характеризують окремі ділянки й особливості обличчя, зокрема, контури носа, губ, брів, відстань між ними тощо. На базі цих відомостей відповідно до загальних принципів біометричних технологій утворюються цифрові моделі ідентифікаторів, які потім порівнюються між собою.

На етапі «навчання» системи використовуються сотні тисяч зображень особи людини під різними кутами, за різних умов освітлення, в сонцезахисних окулярах і без них, з різними зачісками тощо. Під час «навчання» система запам'ятовує процес природного старіння. Особу вдається успішно розпізнати й

у разі зміні ракурсу зйомки (більшість систем допускає поворот на кут до 45°). Утім для отримання гарних результатів потрібна високоякісна відеокамера, бо сканування забирає помітний час (до 30 с).

Надійність роботи системи розпізнавання осіб залежить від декількох чинників [6]:

– якості зображення. Ймовірність безпомилкової роботи системи помітно знижується, якщо людина, котру ідентифікують, дивиться не прямо в камеру, або знято при поганому освітленні;

– актуальності фотографії, доданої до БД;

– обсягу БД.

Технології ідентифікації за обличчям вельми чутливі до зовнішніх умов (поворот голови, кут її нахилу, освітленість тощо) та змін зовнішності людини (макіяж, окуляри, борода). Це призводить до того, що досліджувані технології характеризуються найнижчим відсотком успішного розпізнавання користувачів і водночас найвищим відсотком помилкових спрацьовувань, коли біометрична система помилково приймає одну людину за іншу.

До переваг геометрії обличчя як біометричного ідентифікатора належить безконтактний спосіб отримання відомостей, які необхідні для розпізнавання користувачів, і широкий вибір джерел таких відомостей (фотографії, відеоряд, дані відеоспостереження).

Як приклад ідентифікації за обличчям наведемо продукти фірми Micros (США). Система TrueFace на базі нейронної мережі здатна обробляти кілька зображень обличчя, котрі відрізняються одне від одного поворотом голови чи освітленням. До того ж, система визначає характерні риси по всій ширині (значна частина систем такого типу обмежується вимірюванням відстані і кутів в області очей-носа-рота). З програмою фірми TrueFace CyberWatch Logon95 можуть працювати звичайні ПЕОМ, обладнані вебкамерою, що зафіксована на моніторі. Вартість програми становить близько 100 $. На сучасному ПЕОМ система може порівняти особу за одну секунду, зі швидкістю 500 осіб/с.

Навіть дешеві системи ідентифікації особи за рисами обличчя (витрати на їхню реалізацію не перевищують 50 $) є досить ефективними, оскільки здатні встановити особу людини, навіть якщо вона прикриває півобличчя. Тому такі системи широко використовуються, зокрема, серед провідних казино Лас-Вегаса.

Як ще один приклад розглянемо такий продукт, як біометричний термінал розпізнавання геометрії особи iFace302 вітчизняного виробника ТОВ «Технотрейд. Він виготовлений з процесора Multi Bio 600, інфрачервоної камери з високою роздільною здатністю, 4,3-дюймового TFT-екрана. Термінал містить 700 шаблонів обличчя. Вартість даного зчитувача становить близько 1200 $.

1.4 Висновки до першого розділу

У першому розділі було проаналізовано предметну область. Наведено сучасні принципи розпізнавання обличчя за допомогою систем комп’ютерного зору. Виконано порівняння біометричних ідентифікаторів.

Розглянуто види біометричних систем захисту інформації. Визначено, що системи ідентифікації, котрі аналізують характерні риси особи людини, можна розподілити на дві великі групи: фізіологічні (статистичні характеристики) та поведінкові або психологічні (динамічні характеристики). Проведено порівняльний аналіз можливостей застосування технологій біометричної ідентифікації в системах контролю та керування доступом.

2 СТРУКТУРНЕ ПРОЄКТУВАННЯ СИСТЕМИ ПРОГРАМНОГО КОНТРОЛЮ ДОСТУПУ НА ВИРОБНИЧЕ ПІДПРИЄМСТВО ЗА ТЕХНОЛОГІЄЮ ІДЕНТИФІКАЦІЇ ОСОБИ

2.1 Вибір методів декомпозиції задач під час розпізнавання образів

Для реалізації структурного проєктування будь-якої інформаційної системи необхідно виконати декомпозицію задачі, котру буде реалізовувати проєктована система.

Декомпозицією називають науковий метод, який використовує структуру завдання і дозволяє замінити рішення однієї великої задачі розв’язанням серії менших завдань. При цьому на етапі декомпозиції реалізується закріплення цілей, завдань, критеріїв їхнього досягнення і відповідних числових показників за структурними елементами організації різного ієрархічного рівня. Було розроблено різні підходи декомпозиційних методів [12].

На етапі декомпозиції, що забезпечує загальне уявлення про розв'язувану проблему, виконуються:

– визначення і декомпозиція загальної мети розробки;

– виокремлення проблеми з середовища, визначення її ближнього і далекого оточення;

– опис чинників, які впливають.

Найчастіше декомпозиція виконується шляхом побудови дерева цілей і дерева функцій. Основна проблема при цьому полягає у дотриманні двох суперечливих принципів:

– повноти, де проблема повинна бути розглянута максимально всебічно і докладно;

– простоти, де все дерево повинно бути максимально компактним «вшир» і «вглиб».

Глибина декомпозиції є обмеженою. Якщо під час декомпозиції з’ясовується, що модель починає описувати внутрішній алгоритм функціонування елемента замість закону його функціонування у вигляді «чорного ящика», то в даному разі відбулася зміна рівня абстракції. Це свідчить про вихід за межі мети дослідження системи і, отже, спричиняє припинення декомпозиції. У сучасних методиках типовою є декомпозиція моделі на глибину 5-6 рівнів [12].

У загальній теорії систем доведено, що більшість систем можуть бути декомпозовані на базові уявлення підсистем. До них належать: послідовне (каскадне) з'єднання елементів, паралельне з'єднання елементів, з'єднання за допомогою зворотного зв'язку.

Проблема виконання декомпозиції полягає в тому, що в складних системах відсутня однозначна відповідність між законом функціонування підсистем і алгоритмом, який його реалізує. Тому виконується формування декількох варіантів (або одного варіанту, за умови, що система відображена у вигляді ієрархічної структури) декомпозиції системи.

Найчастіше використовують стратегії декомпозиції:

– функціональна декомпозиція. Декомпозиція ґрунтується на аналізі функцій системи. До того ж, ставиться питання, що робить система, незалежно від того, як вона працює. Підставою розбиття на функціональні підсистеми стає спільність функцій, які реалізуються групами елементів;

– декомпозиція за життєвим циклом. Ознакою виділення підсистем є зміна закону функціонування підсистем на різних етапах циклу існування системи «від народження до загибелі». Для життєвого циклу керування організаційно-економічної системи виділяють такі етапи, як планування, ініціювання, координації, контролю, регулювання. Для інформаційних систем поділяють етапи оброблення інформації: реєстрацію, збір, передавання, оброблення, відображення, зберігання, захист, знищення;

– декомпозиція за фізичним процесом. Ознакою виділення підсистем є кроки виконання алгоритму функціонування підсистеми, стадії зміни станів.

Зважаючи на те, що дана стратегія корисна під час опису існуючих процесів, її результатом здебільшого може стати занадто послідовний опис системи, котра не буде в повній мірі враховувати обмеження, що диктуються функціями один одному. До того ж, може виявитися прихованою послідовність керування. Застосовувати дану стратегію доцільно тільки у разі, якщо метою моделі є опис фізичного процесу як такого [12];

– декомпозиція за підсистемами (структурна декомпозиція). Ознакою виділення підсистем є сильний зв'язок між елементами за однис з типів відношень (зв'язків), які існують у системі (інформаційних, логічних, ієрархічних, енергетичних тощо). Для опису всієї системи повинна бути побудована складова модель, яка об'єднує всі окремі моделі;

– декомпозиція за входами для організаційно-економічних систем. Ознакою виділення підсистем є джерело впливу на систему. Це може бути система вищого рівня чи нижчого, а також істотна середа;

– декомпозиція за типами ресурсів, які споживаються системою. Формальний перелік типів ресурсів складається з енергії, матерії, часу й інформації (для соціальних систем додаються кадри та фінанси);

– декомпозиція за кінцевими продуктами системи. Підставою можуть служити різні види продукту, котрі вироблені системою;

– декомпозиція діяльності людини. Виокремлюють суб'єкт діяльності; об'єкт, на який спрямована діяльність; засоби, що використовуються в процесі діяльності; навколишнє середовище, всі можливі зв'язки між ними.

Під час проєктування програмного засобу використовувалися такі методології.

IDEF0 – це методологія функціонального моделювання. За допомогою наочної графічної мови IDEF0 досліджувана система реалізується перед розробниками й аналітиками у вигляді набору взаємопов'язаних функцій (функціональних блоків – у термінах IDEF0). Зазвичай, моделювання засобами IDEF0 - це перший етап вивчення будь-якої системи. Методологія IDEF0, як правило, застосовується для опису процесів верхнього рівня, втім дозволяє

описати і всю діяльність компанії. Відмінною можливістю нотації вважається можливість відображення не тільки входів і виходів кожного блоку, але й «керування» та «механізмів».

IDEF3 – це методологія документування процесів, які функціонують у системі (на підприємстві), описуються сценарій і послідовність операцій для кожного процесу. IDEF3 має прямий взаємозв'язок із методологією IDEF0: кожна функція (функціональний блок) може реалізовуватися як окремий процес засобами IDEF3 [13].

DFD позначає діаграми потоків даних. Таку номінацію має методологія графічного структурного аналізу, що описує зовнішні по відношенню до системи джерела й адресати даних, логічні функції, потоки даних і сховища даних, до яких виконується доступ.

2.2 Розроблення функціональної моделі системи розпізнавання за технологією ідентифікації особи

У зв’язку з тим, що потрібно розробити структурну діаграму, доцільно використовувати методологію IDEF0. Для цього застосуємо програму Ramus.

Ramus є кросплатформеною системою моделювання й аналізу бізнес-процесів.

Базова функціональність полягає у:

– розробленні графічних моделей бізнес-процесів (підтримуються нотації IDEF0 і DFD);

– розробленні систем класифікації та кодування (з прив'язкою до моделей процесів);

– формуванні звітності відповідно до моделей та систем класифікації (на кшталт регламентів бізнес–процесів, посадових інструкцій тощо).

Переваги перед аналогами полчгають в:

– ергономічності графічного редактора. Редактор підтримує швидку навігацію по моделі, можливість скасування останніх дій, шаблони часто використовуваних типів діаграм, "розумну" поведінку стрілок;

– підтримці необмеженої кількості атрибутів різних типів;

– автоматичній побудові ієрархічних дерев у класифікаторах на підставі значень атрибутів.

Редактор звітів підтримує кілька варіантів налаштувань: спрощений (із використанням інструментів редактора та набору ключових слів) і розширений (із використанням JavaScript). Гнучкий графічний інтерфейс користувача. Шаблони звітів можуть бути експортовані й імпортовані в форматі файлів XML.

Кросплатформеність. Застосування технології Java дозволяє інсталювати систему, зважаючи на різні види операційних систем і апаратних платформ (MS Windows, Mac OS, Linux тощо).

Процес моделювання будь-якої системи в IDEF0 розпочинається з визначення контексту, найбільш абстрактного рівня опису системи в цілому. До контексту входить визначення суб'єкта моделювання, цілі і точки зору на модель.

На рисунку 2.1 подано контекстну діаграму системи програмного контролю доступу на виробниче підприємство за технологією ідентіфікації особи.

На зазначеній діаграмі продемонстровано загальне уявлення про роботу, а також взаємозв'язок із зовнішнім середовищем або іншими процесами.

На вході системи користувач, оскільки сам користувач проходитиме процес сканування та аутентифікації. До виконавчих механізмів можна віднести ПЗ, яке виконуватиме сканування, тренування каскаду та інші процеси, та БД, оскільки в ній зберігаються всі шаблони. Керуючим елементом вказані різні алгоритми, тому що небхідно запрограмувати ПЗ для успішної роботи. На виході отримуємо звіт про надання (або відмову надання) доступу до захищеної інформації.

Рисунок 2.1 – Контекстна діаграма системи програмного контролю доступу на виробниче підприємство за технологією ідентифікації особи

Під час декомпозиції контекстної діаграми отримуємо декомпозицію контекстної діаграми автоматизацій модуля програмного доступу за технологією ідентифікації особи, продемонстровану на рисунку 2.2.

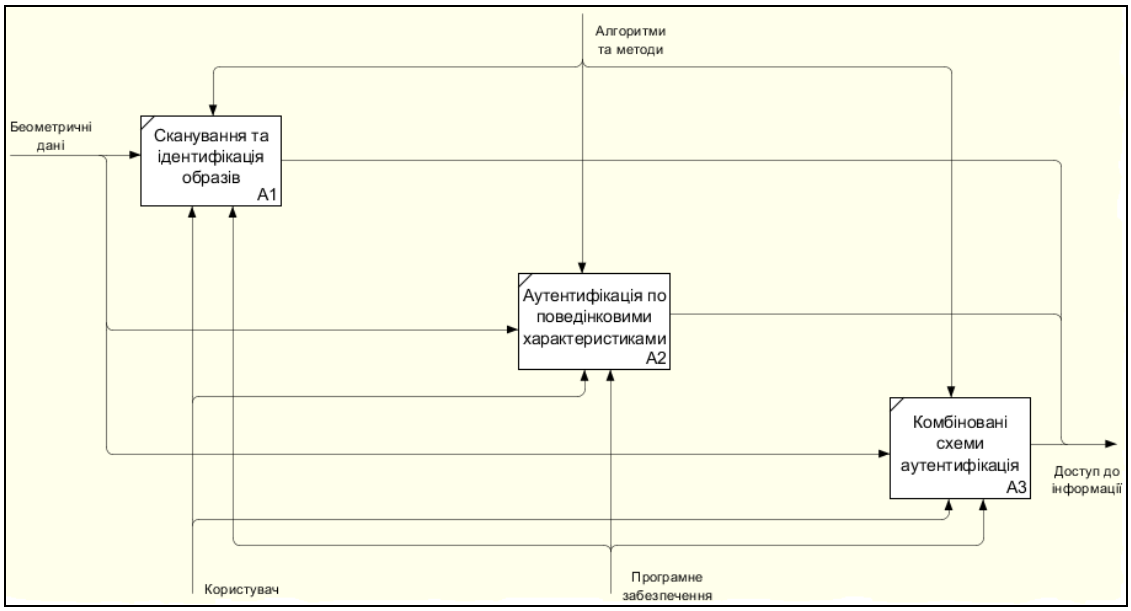

Рисунок 2.2 – Діаграма декомпозиції контекстної діаграми системи програмного доступу на виробниче підприємство за технологією ідентифікації особи

На цьому рівні видно, що перед початком проведення аутентифікації алгоритм необхідно навчити. На виході формується навчений каскад (алгоритм, який спирається на ключові точки образу), за допомогою якого застосунок порівнюватиме дані, котрі надійшли під час аутентифікації з шаблонами, що зберігаються в БД.

На рисунку 2.3 наведено діаграму декомпозиції функції «Сканування та ідентифікація образів», яка надто пов'язана з темою роботи.

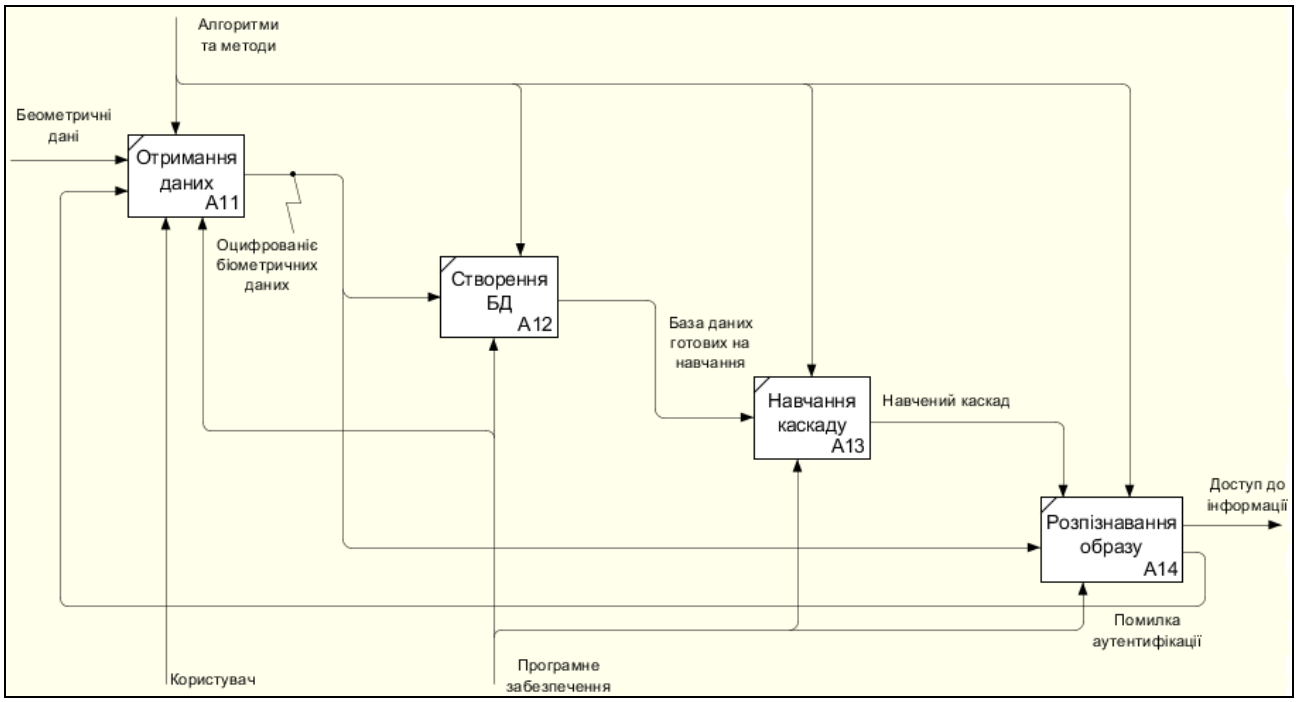

Рисунок 2.3 – Діаграма декомпозиції функції
«Сканування та ідентифікація образів»

Тут продемонстровано приблизний алгоритм роботи застосунку для сканування та розпізнавання образів у біометричних системах захисту інформації. Користувач проходить процес сканування, його дані формуються, здебільшого, у вигляді зображення. Потім ці дані конвертуються в узагальнену форму для проведення розпізнавання. У разі виникнення помилки аутентифікації треба повторити процес спочатку.

2.3 Висновки до другого розділу

У результаті написання другого розділу проведено вибір методів декомпозиції задач під час розпізнавання образів. Наведено принципи застосування IDEF, тобто методології функціонального моделювання програмних засобів. Розроблено функціональну модель системи розпізнавання за технологією ідентифікації особи. Утворено діаграму декомпозиції функції «Сканування та ідентифікація образів».

3 РОЗРОБЛЕННЯ ПРОГРАМНОГО КОНТРОЛЮ ДОСТУПУ НА ВИРОБНИЧЕ ПІДПРИЄМСТВО ЗА ТЕХНОЛОГІЄЮ ІДЕНТИФІКАЦІЇ ОСОБИ

3.1 Використані у роботі засоби та методи

Бібліотека мови Python, яка підтримує великі багатовимірні масиви та матриці, взаємодіє з великою бібліотекою високорівневих і математичних функцій для операцій з цими масивами, котрі працюють достатньо швидко за рахунок використання вставок на мовах: C, C ++.

Бібліотека Dlib. Бібліотека алгоритмів машинного навчання і різних додаткових допоміжних інструментів. З цієї бібліотеки застосовується готова навчена модель AAM (Active Appearance Model) для знаходження лицьових точок.

Бібліотека OpenFace. Відкрита бібліотека для розпізнавання осіб, яка застосовує глибоку згортальну нейронну мережу, котра заснована на технології FaceNet.

Бібліотека OpenCV. Бібліотека алгоритмів комп'ютерного зору, оброблення зображень та чисельних алгоритмів загального призначення з відкритим кодом.

У данній роботі було застосовано бібліотеку OpenCV, оскільки вона підтримує найбільшу кількість мов програмування, налічує велику кількість прикладів, багату функціональну базу та легко інтегрується з середовищем розробки MicrosoftVisualStudio.

У даній роботі з бібліотеки OpenCV було використано такі засоби [11]:

– методи розпізнавання обличчя (EigenFaces, FisherFaces, LBPH);

–метод Віоли-Джонса з метою детектування образів;

– інші різні функції для перетворення зображень.

Метод Віоли-Джонса для детектування осіб [15].

У 2001 році Віола і Джонс запропонували алгоритм, котрий став проривом в області розпізнавання облич. Метод використовує технологію ковзного вікна. Тобто рамка, що має розмір, менший за вихідне зображення, рухається з деяким кроком по зображенню, і за допомогою каскаду слабких класифікаторів визначає, чи присутні обличчя в даному вікні. Метод змінного вікна ефективно використовується в різних завданнях комп'ютерного зору.

Метод складається з двох підалгоритмів: алгоритму навчання й алгоритму розпізнавання. На практиці швидкість роботи алгоритму навчання не важлива. Вкрай важлива швидкість роботи алгоритму розпізнавання. За вивченої раніше класифікації можна відрізняти структурні, статистичні та нейронні методи.

Метод налічує такі переваги:

– ймовірність знаходити більше однієї особи на зображенні;

– застосування простих класифікаторів демонструє хорошу швидкість і дозволяє використовувати цей метод у потоці.

Утім метод складно навчати, оскільки для навчання потрібна велика кількість тестових даних, а також передбачається тривалий час навчання, котрий вимірюється днями.

Спочатку алгоритм був запропонований для розпізнавання тільки облич, утім ним можна послуговуватись і для розпізнавання інших об'єктів. Одним із внесків Віоли і Джонса було застосування таблиці сум (інтегральне зображення).

Параметрами для алгоритму розпізнавання автори запропонували обрати ознаки Хаара, на основі вейвлетів Хаара (угорського математика Альфреда Хаара).

У задачі щодо розпізнавання облич загальне спостереження виявило, що серед всіх облич області очей темніші за області щік. Розглянемо маски, що складаються зі світлих і темних областей. Кожна маска характеризується розміром світлої і темної областей, пропорціями, а також мінімальним розміром. Разом з іншими спостереженнями були запропоновані такі ознаки

Хаара (рис. 3.1), як простір ознак у задачі розпізнавання для класу облич.

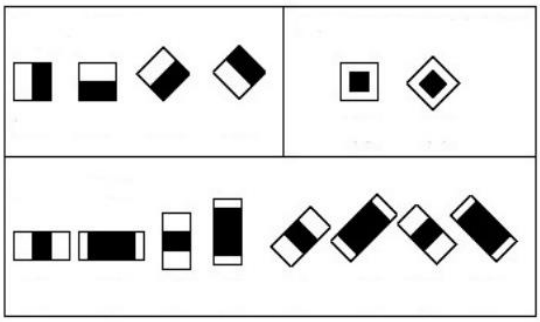

Рисунок 3.1 – Набір ознак Хаара у методі Віоли-Джонса

Ознаки Хаара дають точкове значення перепаду яскравості по осі X і Y відповідно. Таким чином, загальна ознака Хаара для розпізнавання осіб подається як набір двох суміжних прямокутників, які лежать вище очей і на щоках. Значення ознаки обчислюється за формулою:

$$F = X - Y \tag{3.1}$$

де X – сума значень яскравості точок закриваються світлою частиною ознаки;

Y – сума значень яскравості точок закриваються темною частиною ознаки.

Виходить, що якщо вираховувати суми значень інтенсивностей для кожної ознаки, то це потребуватиме значних обчислювальних ресурсів. Віолою і Джонсом було запропоновано використовувати інтегральне представлення зображення (докладніше про нього буде згадано далі). Таке уявлення стало досить зручним способом обчислення ознак і, відповідно, також почало застосовуватися в інших алгоритмах комп'ютерного зору, наприклад SURF. Навчання алгоритму Віола–Джонса трактується як навчання алгоритму з учителем.

Метод EigenFaces [16]. Основний підхід цього методу полягає у стисненні інформації вихідного зображення без істотних втрат інформативності за допомогою методу головних компонент (PCA). Припустимо, що існує база

даних осіб, в якій зображення мають розмір $N \times N$ пікселів. Кожне зображення з бази даних представляють точкою в просторі розмірністю $N \times N$. Основною ідеєю алгоритму стає пошук такого базису меншої розмірності, після проекції в якому максимально зберігатиметься інформація по осях з великою дисперсією і втрачатиметься інформація по осях з маленькою дисперсією. Це потрібно для того, щоб залишити лише ту інформацію, котра б характеризувала відмінності осіб, і видалити непотрібну інформацію, котра може перешкодити правильно ідентифікувати людину.

Процедура ідентифікації реалізується в новому базисі з використанням евклідової метрики.

Основні недоліки алгоритму EigenFaces полягають у відсутності стійкості до зміни умов освітленості, а також відсутності інваріантності до афінних перетворень.

Метод LBPH [17]. Вчені вирішили спробувати витягувати ознаки з країв зображення. Такий набір ознак має маломірну структуру, що вважається позитивною рисою даного методу. Зважаючи на те, що ознаки витягуються з країв, це дозволяє бути алгоритму стійким до масштабу, поворотів тощо.

Опис роботи методу LBPH: спершу зображення поділяється на однакові блоки, що утворюють сітку (рис. 3.2). Далі для кожного блоку будується гістограма кодів, які обчислюються таким чином: береться піксель, який порівнюється із сусідами, якщо інтенсивність центрального пікселя є більшою чи дорівнює інтенсивності сусіда, то він позначається 1, інакше – 0. У результаті кожного пікселя буде відповідати двійкове число, що складається з результатів порівнянь. Отримані гістограми об'єднуються в одну загальну, котра є підсумковим дескриптором, який застосовується для класифікації особи [16].

Описаний підхід дозволяє охоплювати дуже дрібнозернисті деталі. Згодом виявилося, що LBPH не міг кодувати деталі різного масштабу. У зв’язку з цим його було розширено. Таким чином, наразі число сусідів може варіюватися.

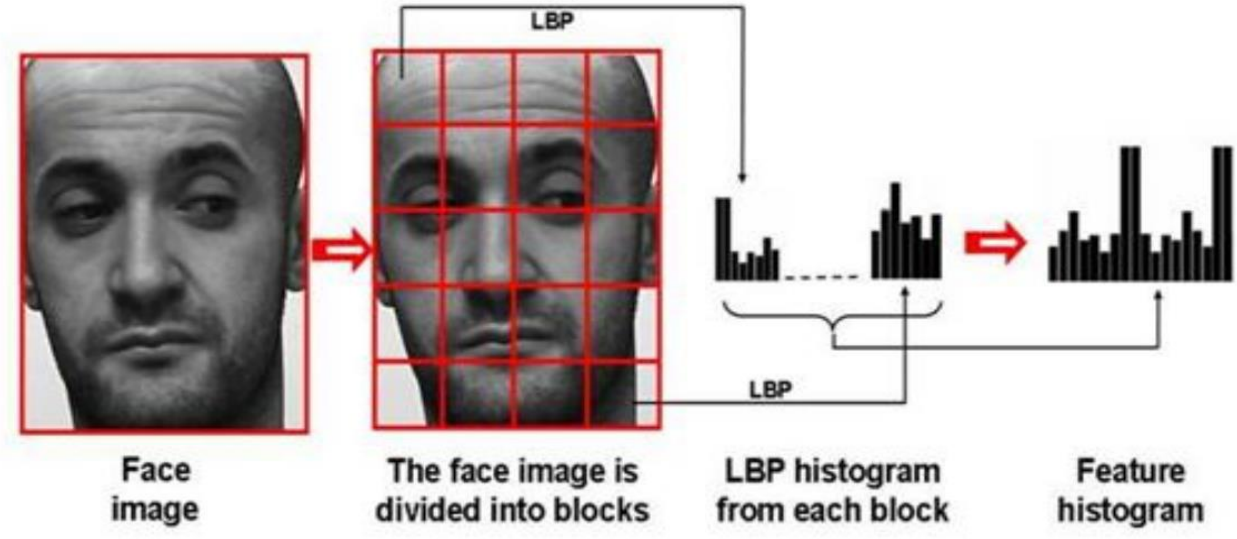

Рисунок 3.2 – Схема роботи алгоритму LBPH

Технологія FaceNet [18]. Технологія Google була опублікована в 2015 році. Вона розроблена Флоріаном Шрофом, Дмитром Калиниченком та Джеймсом Філібіном.

Для розпізнавання застосовується навчена глибока згортальна нейронна мережа, котра повертає 128-розмірний вектор ознак, а також відмінно класифікується. Евклідова відстань стала актуальною для метрики схожості осіб. Хоча дана технологія по праву вважається на сьогодні найточнішою, проте вона є власністю Google, отже, її застосування в даній роботі не є можливим.

Метод FisherFaces [18]. Алгоритм передбачає наявність безлічі фотографій за різних умов освітленості у кожної персони в базі даних. В алгоритмі, як і в EigenFaces, передбачається пошук базису, проте такого, що дозволив би максимізувати дисперсію між множинами зображень облич і одночасно мінімізувати дисперсію всередині кожної безлічі.

Відомо, що компоненти, що було визначено за допомогою PCA, не завжди містять в собі всю відмінну інформацію. З огляду на це зразки різних класів змішуються один з одним, а подальша класифікація стає неможливою. Цю проблему вирішує алгоритм LDA (Лінійний дискримінантний аналіз), який

є основою методу FisherFaces [18].

LDA є методом статистики та машинного навчання, що застосовується для пошуку лінійних комбінацій ознак, найкращим чином розділяють два або більше класів об'єктів або подій (тобто об'єкти одного і того ж класу повинні знаходитися якомога ближче один до одного в просторі, і при цьому відбувається максимізація відстані між класами). Отримана комбінація може бути використана як лінійний класифікатор або для скорочення розмірності простору ознак перед наступною класифікацією.

У даній роботі було вибрано та реалізовано саме цей метод, тому що в порівнянні з іншими методами під час роботи на базі тестових зображень [18] він дає найкращий результат і за точністю і за швидкодією (не враховуючи технології FaceNet).

Результат цих порівнянь продемонстровано на рисунках 3.3-3.4.

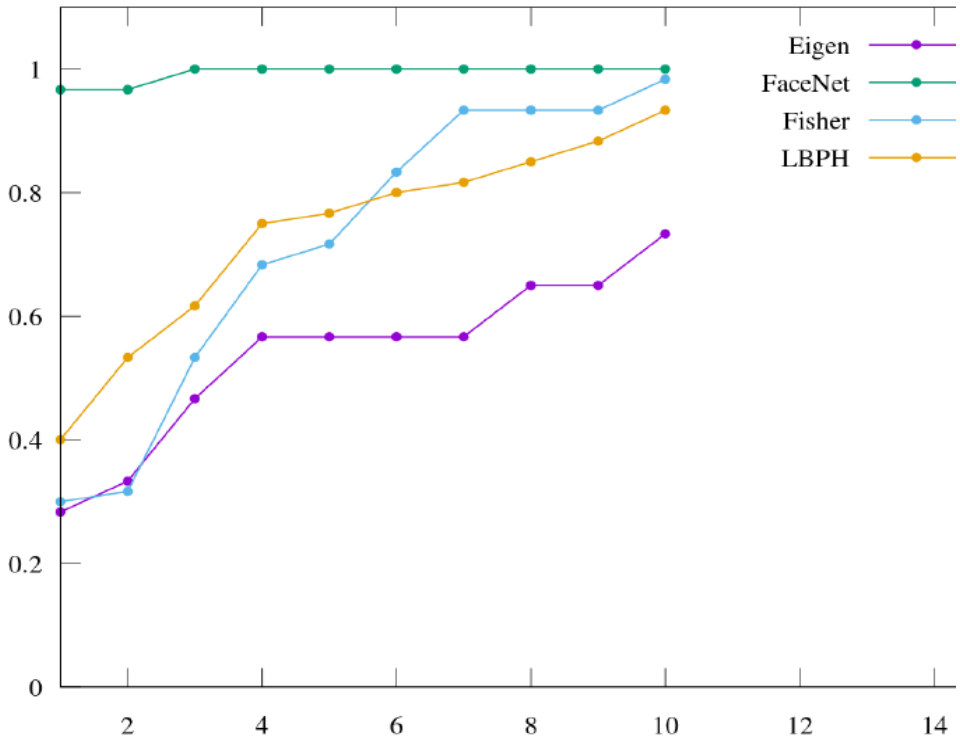

Рисунок 3.3 – Графік порівняння точності роботи алгоритмів на базі GeorgiaTechFaceDatabase

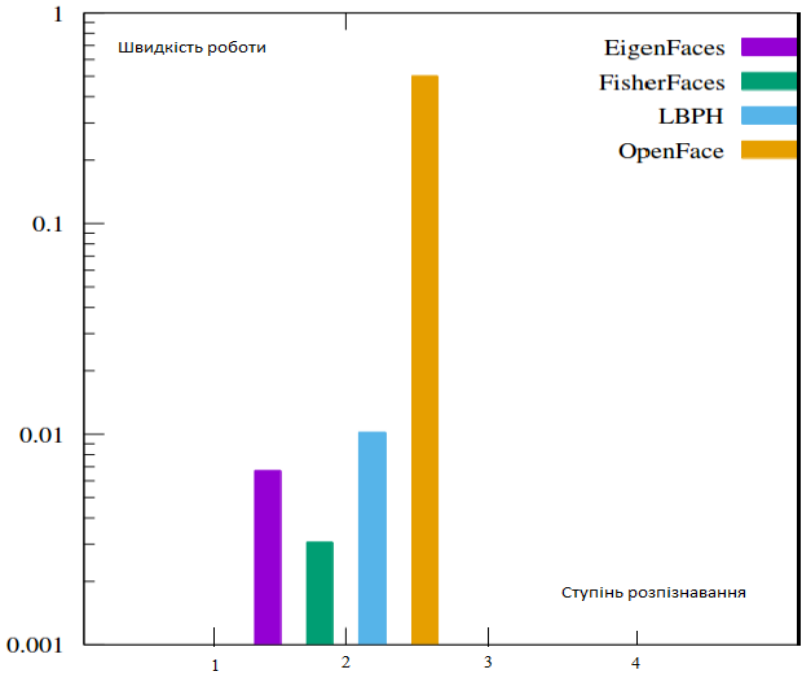

Рисунок 3.4 – Графік порівняння швидкості роботи алгоритмів на базі GeorgiaTechFaceDatabase

3.2 Вибір середовища розробки

Microsoft Visual Studio 2017 є набором інструментів для створення програмного забезпечення: від планування до розроблення призначеного для користувача інтерфейсу, написання коду, тестування, налагодження, аналізу якості коду та продуктивності, розгортання в середовищах клієнтів, а також збору даних телеметрії щодо використання. Перелічені інструменти призначені для максимально ефективної спільної роботи. Вони є доступними в інтегрованому середовищі розробки (IDE) Visual Studio.

Visual Studio можна використовувати для створення різних типів застосунків [19], зокрема, від простих застосунків для магазину та ігор для мобільних клієнтів до великих і складних систем, які обслуговують підприємства та центри оброблення даних. Користувачі можуть створювати:

– застосунки та ігри, що створюються не тільки на платформі Windows, але і на Android і iOS;

– вебсайти і вебслужби на базі ASP.NET, JQuery, AngularJS і інших

популярних платформ;

– застосунки для різноманітних платформ і пристроїв, включно, втім не обмежуючись: Office, Sharepoint, Hololens, Kinect і "Інтернету речей";

– ігри та графічні застосунки для різних пристроїв Windows, включно з Xbox, з підтримкою DirectX.

За замовчуванням Visual Studio забезпечує підтримку C#, C і C++, JavaScript, F# і Visual Basic.

C++ є компільованою, статично типізованою мовою програмування загального призначення.

Підтримує такі парадигми програмування, як процедурне, об'єктно–орієнтоване, а також узагальнене програмування. Мова містить багату стандартну бібліотеку, до складу якої входять: поширені контейнери й алгоритми, введення-виведення, регулярні вирази, підтримку багатопоточності й інші можливості. C++ поєднує властивості як високорівневих, так і низькорівневих мов. У порівнянні з її попередником – мовою C, – найбільшу увагу приділено підтримці об'єктно-орієнтованого й узагальненого програмування.

C++ активно використовується для розроблення програмного забезпечення, тому стала однією з найпопулярніших мов програмування. Область її застосування розповсюджується на створення операційних систем, різноманітних прикладних програм, застосунків для вбудованих систем, драйверів пристроїв, високопродуктивних серверів, а також розважальних програм (ігор). Існує безліч реалізацій мови C++, як безкоштовних, так і комерційних. До того ж для різних платформ: GCC, Visual C++, Intel C++ Compiler, Embarcadero (Borland) C++ Builder тощо. C++ набула величезного впливу на інші мови програмування, перш за все на Java і C#.

Синтаксис C++ успадкований від мови C. Одним з принципів розроблення стало збереження сумісності з C. Однак C++ не є в строгому сенсі різноманітністю C. Програм, які можуть однаково успішно транслюватися як компіляторами C, так і компіляторами C++ - безліч, утім не містять всі можливі

програми на С.

У даній роботі було використувано саме її, оскільки ця мова підтримується у вибраному середовищі розробки, має багато корисних функцій для полегшення процесу програмування, інтегрування зі сторонніми бібліотеками та поєднується з різноманітними пристроями.

3.3 Розроблення алгоритму програми

Цей програмний засіб призначений для демонстрації роботи алгоритмів сканування та розпізнавання обличчя за допомогою ознак Хаара, а також навчання визначальних каскадів та подальшого їхнього застосування. На рисунку 3.5 подано загальний алгоритм роботи програми.

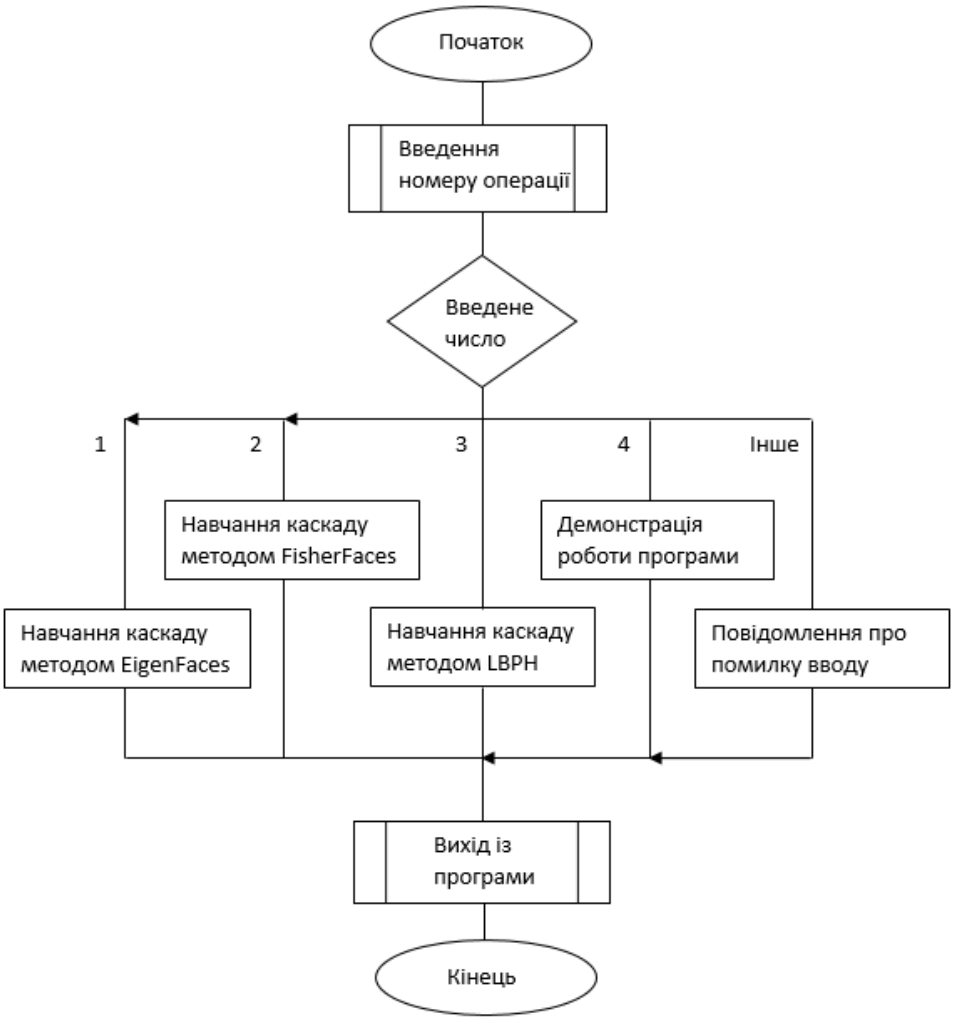

Рисунок 3.5 – Схема загального алгоритму роботи розробленої програми

На рисунку 3.6 продемонстровано більш детальний алгоритм роботи частини програми, котра відповідає за сканування та розпізнавання обличчя (ініціюється введенням числа 4 на початку роботи програми).

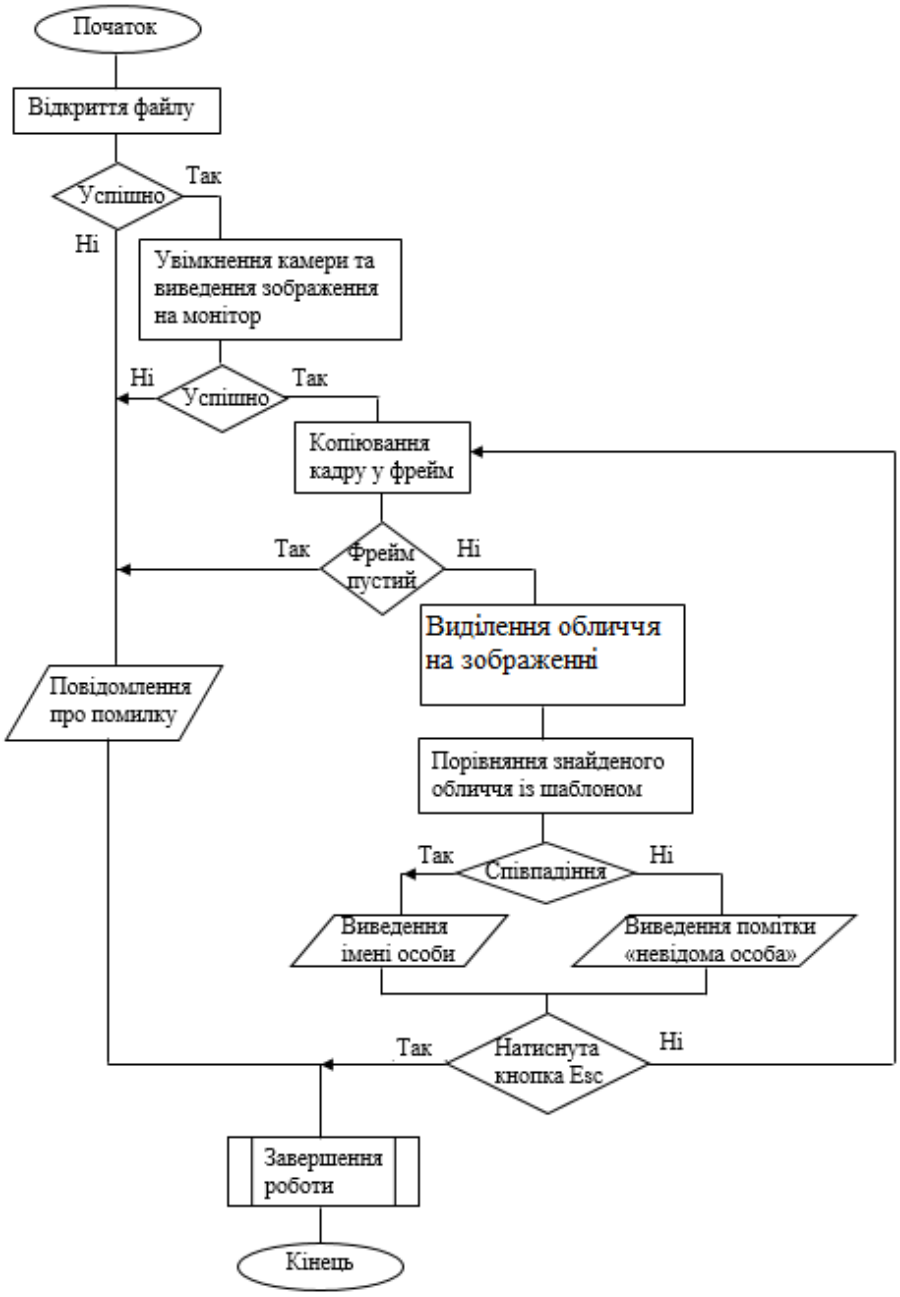

Рисунок 3.6 – Схема алгоритму роботи программи розпізнавання обличчя

Программа спершу перевіряє можливість підключення файлу навченного каскаду та увімкнення вебкамери. Якщо є можливість, то виводить зображення з камери на екран, позначає знайдені обличчя та підписує їх за результатами

розпізнавання.

3.4 Алгоритм налаштування й експлуатації програми

Дана програма використовує спеціальну бібліотеку комп'ютерного зору OpenCV [11]. OpenCV (англ. Open Source Computer Vision Library - бібліотека комп'ютерного зору з відкритим вихідним кодом) – бібліотека алгоритмів комп'ютерного зору, оброблення зображень та чисельних алгоритмів загального призначення з відкритим кодом. Реалізована на C / C ++. Крім того, розробляється для Python, Java, Ruby, Matlab, Lua та інших мов. Може вільно реалізовуватись в академічних і комерційних цілях – поширюється в умовах ліцензії BSD.

Для затвердження загального стандартного інтерфейсу комп'ютерного зору і застосунків в цій області. Для сприяння зростанню числа таких застосунків і створення нових моделей використання PC.

Зробити платформи Intel привабливими для розробників таких застосунків за рахунок додаткового прискорення OpenCV за допомогою Intel® Performance Libraries (зараз містять IPP - низькорівневі бібліотеки для оброблення сигналів, зображень, а також медіакодеки) та MKL (спеціальну версію LAPACK і FFTPack). OpenCV автоматично визначає присутність IPP і MKL, а також використовує їх для прискорення оброблення.

Підтримувані платформи та інструмент власне бібліотеки:

– Microsoft Windows: компілятори Microsoft Visual C ++ (6.0, .NET 2003), Intel Compiler, Borland C ++, Mingw (GCC 3.x);

– Windows RT: портовано на ARM компанією Itseez;

– Linux: GCC (2.9x, 3.x), Intel Compiler: «./configure-make-make install», RPM (spec файл внесено до постачання);

– Mac OS X: GCC (3.x, 4.x);

– Android;

– iOS.

Використовуються C і «полегшений» C ++. Дуже обмежено використовуються прагма й умовна компіляція.

Засоби GUI, охоплює відео:

– Microsoft Windows: DirectShow, VfW, MIL, CMU1394;

– Linux: V4L2, DC1394, FFMPEG;

– Mac OS X: QuickTime.

У версії 2.2 бібліотека набула реорганізації. Замість універсальних модулів cxcore, cvaux, highGUI та інших було створено кілька компактних модулів із більш вузькою спеціалізацією:

– opencv_core – ключова функціональність. Містить базові структури, обчислення (математичні функції, генератори випадкових чисел), а також лінійну алгебру, DFT, DCT, введення/виведення для XML і YAML тощо;

– opencv_imgproc – оброблення зображень (геометричні перетворення, перетворення колірних просторів, фільтрація тощо);

– opencv_highgui – простий UI, введення / виведення зображень і відео;

– opencv_ml – моделі машинного навчання (SVM, дерева рішень, навчання зі стимулюванням тощо);

– opencv_features2d – розпізнавання й опис плоских примітивів (SURF, FAST тощо, включно зі спеціалізованим фреймворком);

– opencv_video – аналіз руху та відстеження об'єктів (шаблони рухів, оптичний потік, усунення фону);

– opencv_objdetect – виявлення об'єктів на зображенні (перебування осіб за допомогою алгоритму Віоли-Джонса, розпізнавання людей HOG тощо);

– opencv_calib3d – калібрування камери, пошук стереовідповідності, наявність елементів оброблення тривимірних даних;

– opencv_flann – бібліотека швидкого пошуку найближчих сусідів (FLANN 1.5) і обгортки OpenCV;

– opencv_contrib – супутній код, який ще не готовий для функціонування;

– opencv_legacy – застарілий код, який збережений задля зворотної сумісності;

– opencv_gpu – прискорення деяких функцій OpenCV, використовуючи CUDA, створений за підтримки NVidia.

Перед початком роботи необхідно активувати зазначену бібліотеку. Спершу потрібно додати запис у вкладці «Змінні середовища» (рис. 3.7), котра міститься у властивостях системи. Іншими словами має номінацію «Простір імен». Це потрібно для полегшення програмного доступу застосунку до даної бібліотеки.

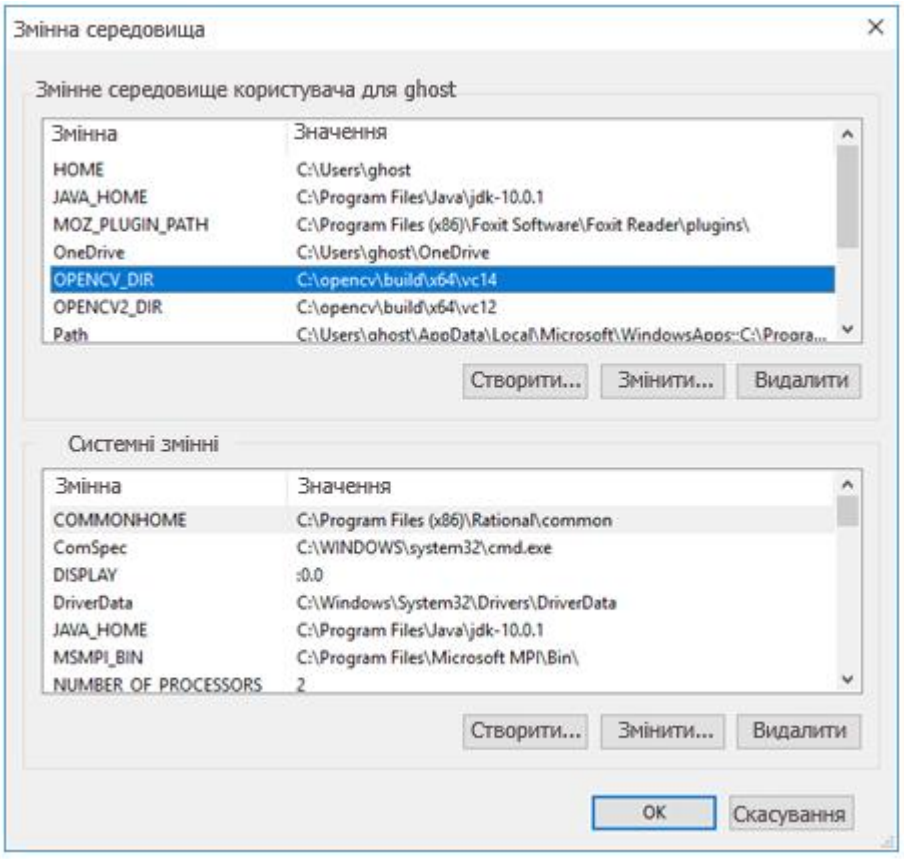

Рисунок 3.7 – Приклад запису у просторі імен

Після активації можна створювати проєкт у вибраному середовищі розробки. У дипломній роботі таким середовищем є Microsoft Visual Studio 2017.

Після створення пустого проєкту у його характеристиках треба зазначити додаткові каталоги додаваємих файлів, додаткові каталоги бібліотек та додаткові залежності, як продемонстровано на рисунках 3.9-3.11. Крім того, під

час програмування необхідно не забути програмно підключити, за потреби, додаткові модулі бібліотеки (рис. 3.8).

```
1   #include "opencv2/core/core.hpp"
2   #include "opencv2/contrib/contrib.hpp"
3   #include "opencv2/highgui/highgui.hpp"
4   #include "opencv2/imgproc/imgproc.hpp"
5   #include "opencv2/objdetect/objdetect.hpp"
6   #include <iostream>
7   #include <conio.h>
8   #include <fstream>
9   #include <sstream>
```

Рисунок 3.8 – Приклад програмного підключення бібліотеки

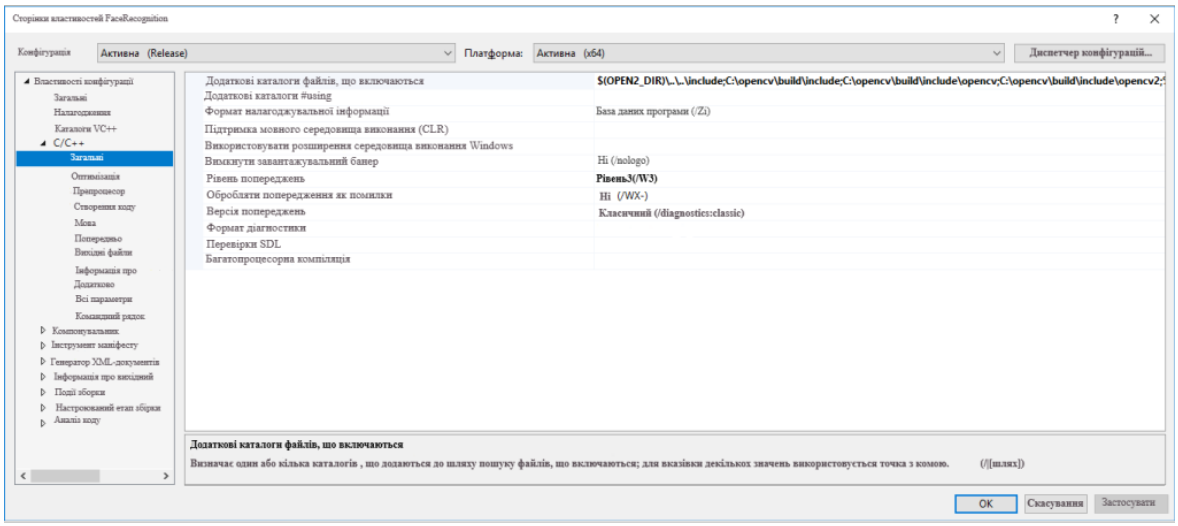

Рисунок 3.9 – Приклад додаткових каталогів доданих файлів

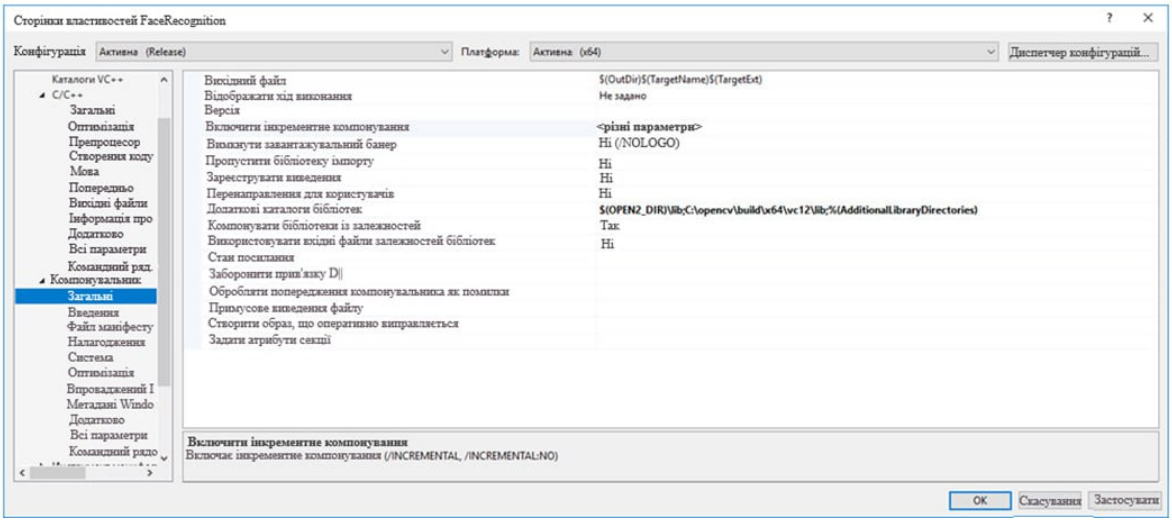

Рисунок 3.10 – Приклад додаткових каталогів бібліотек

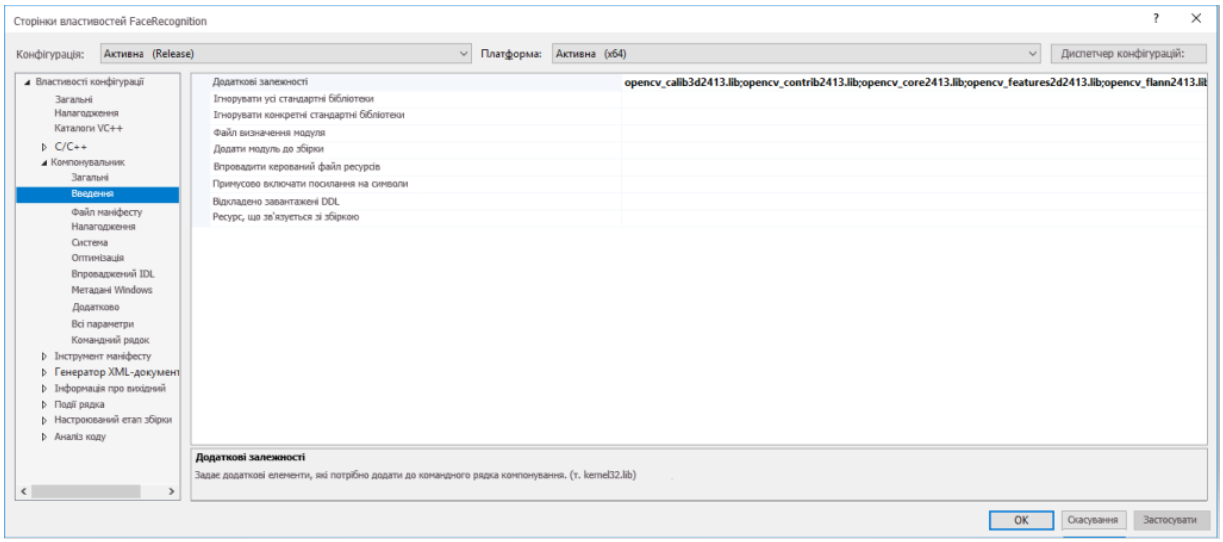

Рисунок 3.11 – Приклад додаткових залежностей

Пошук обличчя на зображенні та порівняння його із шаблоном виконують вбудовані функції бібліотеки OpenCVdetectMultiScale та predict (текст програми подано у додатку А). Частина програми, що реалізує розпізнавання, послуговується методом FisherFaces, оскільки у разі обмеження ресурсів він демонструє найліпший результат. Для стабільної та безперебійної роботи програма вимагає подальшого доопрацювання та навчання, тому що для цього необхідна укомплектована база зображень на десятки тисяч одиниць позитивних та негативних прикладів. Звичайні, домашні ПК, для такого завдання не дуже підготовлені. Аргументуємо, що для даної роботи було використано базу з 4212 негативних і 1813 позитивних прикладів, а час навчання тривав більше 18 годин.

Програма виконана у вигляді консольного застосунку, тому особливих графічних вимог вона не має, втім для коректної роботи програми на ПК повинна бути встановлена система з тактовою частотою 64 біта (не нижче ніж Windows 7). До того ж, мають бути вільними не менше ніж 1Гб оперативної пам'яті і 512 Мб пам'яті відеокарти.

3.5 Розроблення програмного забезпечення

3.5.1 Призначення і умови застосування

Розроблений програмний застосунок призначений для збільшення безпеки особистих даних як на домашніх ПК, так і на корпоративних ЕОМ. Крім того, даний застосунок також може бути корисним для ідентифікації чи спостереження. Для використання цього програмного продукту необхідно мати в наявності комп'ютер із мінімальними системними вимогами, котрі подані у наступному розділі. До того ж має бути фахівець, який вміє налаштовувати подібного роду програми на ПК, за замовчуванням, не призначених для подібних завдань.

3.5.2 Підготовка до роботи

Для роботи програми достатньо мінімальних ресурсів:

– процесора Intel Core I3, або AMD схожої продуктивності;

– обсягу оперативної пам'яті – 1 Гбайт;

– жорсткого диску обсягом вільного простору не менше 2 Гбайт;

– рекомендовано монітор типу VGA або кращого дозволу;

– клавіатури, миші;

– вебкамери з роздільною здатністю не менш 1024×768;

– необхідно також, щоб на ПК було встановлено ПО: ОС сімейства Windows починаючи з Windows 7, Net Framework 4.

Установлення, налаштування програми та підключення додаткової бібліотеки комп’ютерного зору OpenCV повинен виконувати фахівець, який знає що робити та має відповідний досвід.

3.5.3 Опис операцій

Для початку роботи із застосунком потрібно 2 рази натиснути лівою кнопкою миші на ярлик програми (файл з розширенням «.exe»). Після цього з'явиться консольне вікно, як зображено на рисунку 3.12.

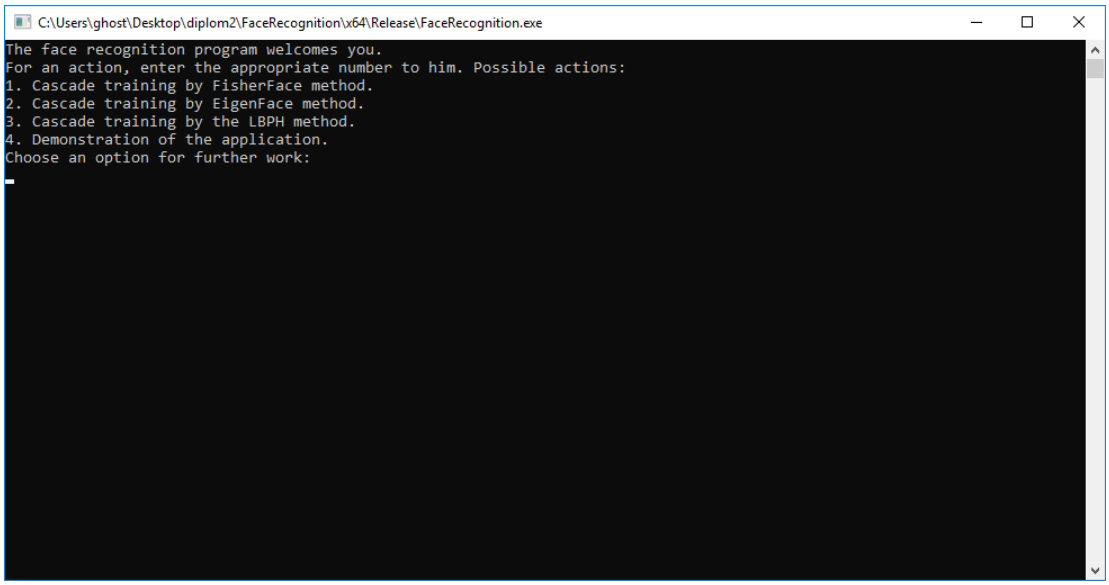

Рисунок 3.12 – Консольне вікно програми

Перед тим, як запускати навчання, треба створити БД зображень користувача. Вони повинні бути у градаціях сірого та мати єдиний розмір. У цьому допоможе додаткова програма, котра за допомогою вебкамери знаходить обличчя і зберігає його у встановленому каталозі.

Після створення бази зображень (рис. 3.13) може бути активовано навчання за одним із вказаних у консольному вікні методів. Для обрання методу треба ввести його номер та натиснути «Enter» (рисунки 3.14-3.16). Чим більше зображень у базі, тим точніше буде результат, однак навчання триватиме довше (у даному випадку це 18 годин).

Рисунок 3.13 – Приклад створеної бази зображень

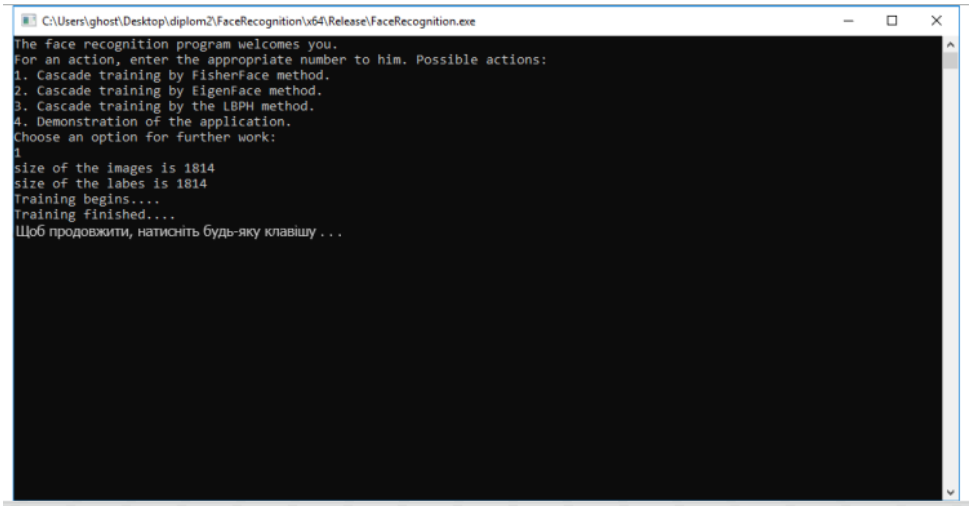

Рисунок 3.14 – Приклад навчання методом FisherFaces

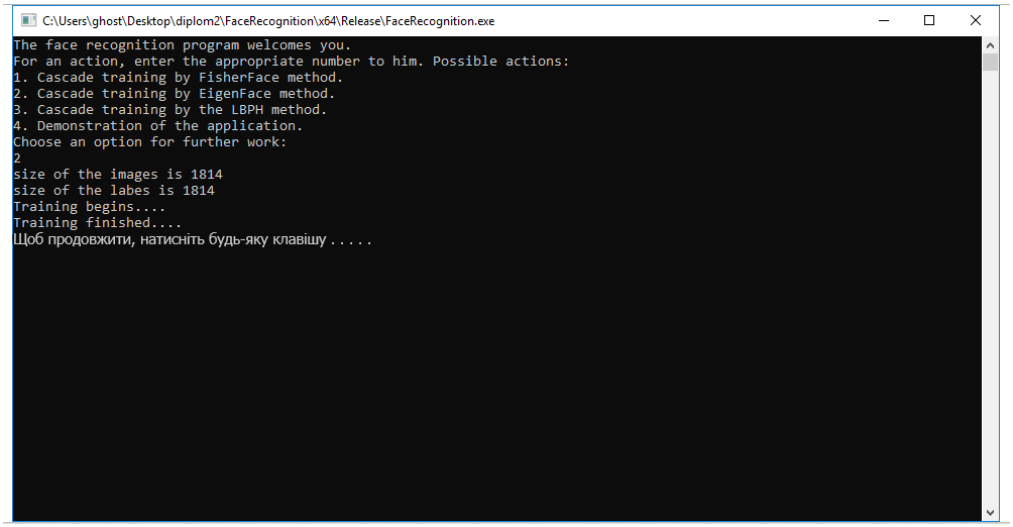

Рисунок 3.15 – Приклад навчання методом EigenFaces

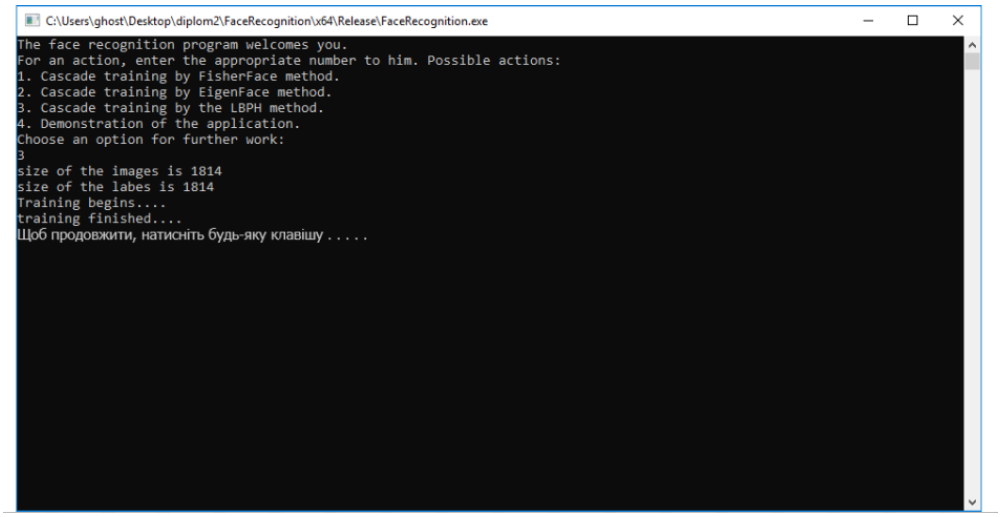

Рисунок 3.16 – Приклад навчання методом LBPH

Для подальшої роботи треба перезапустити програму. Для цього треби вийти з неї, натиснувши клавішу «Esc», або на червону кнопку у правому верхньому куті.

При введенні числа 4 буде створено додаткове вікно, на яке буде виводитись зображення з вебкамери та позначатись знайдені обличчя та підписуватися, чи є серед них обличчя користувача (рис. 3.17).

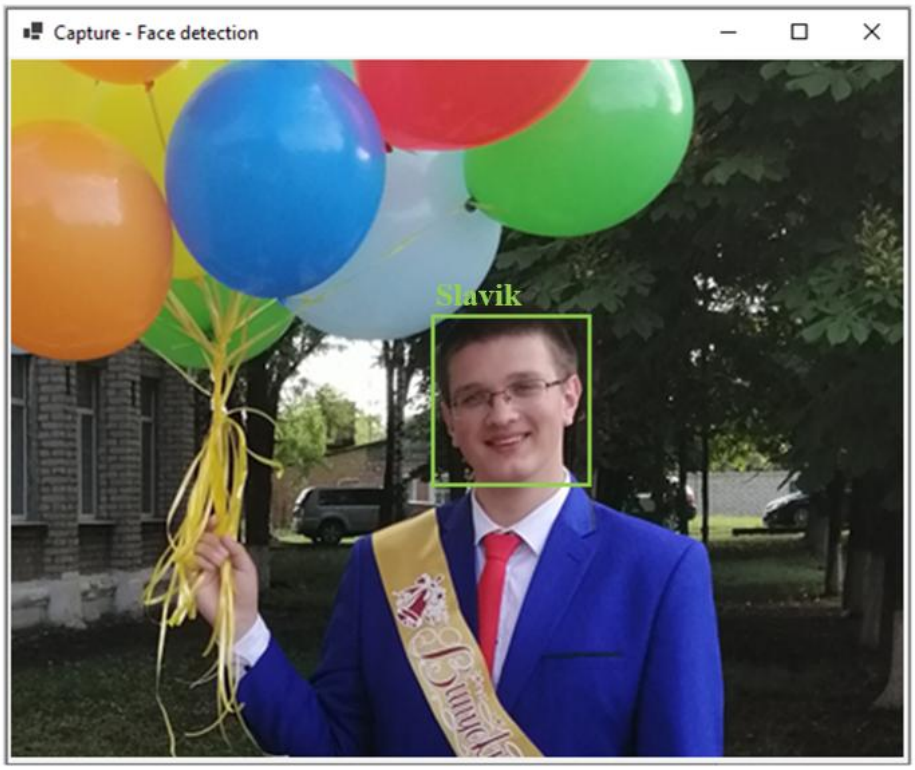

Рисунок 3.17 – Результат роботи програми

3.5.4 Аварійні ситуації

Під час роботи даного застосунку можуть виникнути такі помилки:

– неможливість підключення вебкамери;

– неналаштована додаткова бібліотека OpenCV;

– неможливість відкрити навчений каскад;

– неможливість знайти чи обробити базу зображень для навчання;

– введено не вказане для вибору число (рис. 3.18).

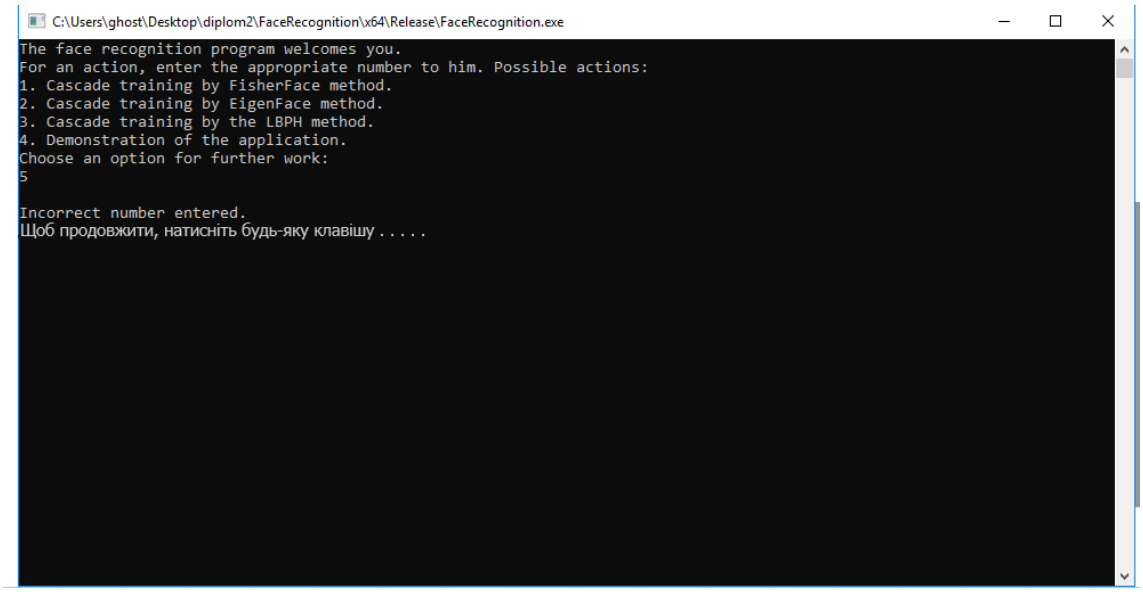

Рисунок 3.18 – Приклад неправильного введення пункту подальшої роботи програми

3.5.5 Рекомендації щодо використання

Для використання даного застосунку розглянемо приклад навчання алгоритму та подальшого перегляду результатів роботи.

Запускаємо застосунок, 2 рази натискаємо лівою кнопкою миші на файл із розширенням «.exe». Відкривається консольне вікно, можно було вже побачити на рисунку 3.12. Обираємо пункт 4, щоб упевнитися, що програма працездатна та може знаходити обличчя. Як видно на рисунку 3.19, програма може знаходити обличчя, втім не розпізнає їх.

Для навчання треба створити базу зображень користувача з дотримуванням умов (рис. 3.13), та вибрати один із методів навчання. Для прикладу було обрано метод FisherFaces (рис. 3.14). Навчання проходить дуже повільно, тому треба мати багато терпіння чи дуже потужний ПК.

Після завершення навчання програму треба перезапустити. Після перезапуску слід обрати пункт демонстрації роботи програми (ввести число 4).

Експериметнальним методом визначили точність розпізнавання, що становить 70 %. Із 500 експериментів 350 виявилися точно розпізнаними.

Імовірність помилки розпізнавання становить 30 %.

Таблиця 3.1 – результати експериментальних апробацій програми

Номер експеримента	Кількість кадрів	Правильно розпізнані	Помилково розпізнані	Не розпізнані
1 (окуляри)	100	82	0	18
2 (капелюх)	130	103	4	23
3 (зачіска)	120	110	0	10

Як видно з таблиці 3.1, експерименти підтверджують, що ймовірність успішного розпізнавання становить 70 %.

Розрахуємо ймовірність успішних розпізнавань:

$$P_1(A) = \frac{82}{100} = 0.82,$$

$$P_2(A) = \frac{103}{130} = 0.79,$$

$$P_3(A) = \frac{110}{120} = 0.91.$$

Розрахуємо ймовірність успішного розпізнавання розробленим програмним модулем:

$$P(A) = \frac{P_1(A) + P_2(A) + P_3(A)}{3} = 0.84.$$

Розрахуємо ймовірність помилки:

$$P\ (\overline{A}) = 1 - P(A) = 0.16.$$

3.6 Висновки до третього розділу

За результатами написання третього розділу роботи виконано розроблення проєктного рішення системи модуля програмного контролю доступу за технологією ідентифікації особи. Для розроблення обрано бібліотеку Dlib мови програмування Python.

Середовищем розробки обрано Microsoft Visual Studio 2017. Розроблено алгоритм роботи програми, алгоритми налаштування й експлуатації програми. Дана програма використовує спеціальну бібліотеку комп'ютерного зору OpenCV. Розроблено графічний інтерфейс та виконано перевірку працездатності програмного засобу.

Розглянуто аварійні ситуації та проведено аналіз отриманих результатів. Експериметнальним методом визначили точність розпізнавання, що становить 70 %. Із 500 експериментів 350 виявилися точно розпізнаними. Ймовірність помилки розпізнавання становить 30 %.

4 ОХОРОНА ПРАЦІ

4.1 Аналіз умов праці на робочому місці

На робочому місці оператора ПК виникають небезпечні та шкідливі чинники: підвищений рівень шуму, несприятливі мікрокліматичні умови, недостатній рівень освітленості, шкідливі речовини, підвищений рівень електромагнітних випромінювань радіочастот, висока напруга електричної мережі, статична електрика тощо. Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. У разі систематичного впливу виробничих чинників, які не відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працівників та можуть виникнути професійні захворювання органів зору, руху, нервової системи. Отже, вивчення умов праці на робочому місці програміста є необхідною умовою запобігання негативних наслідків впливу небезпечних та шкідливих чинників.

Організація робочого місця. Приміщення, в якому знаходиться робоче місце програміста, загальною площею 48 м^2, і висотою стелі 3.5 м. У приміщенні розташовано 6 робочих місць з ПК. Кожне робоче місце обладнане робочим столом, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші.

4.2 Промислова безпека на робочому місці

Живлення ПК здійснюється від трифазної електричної мережі змінного струму з глухозаземленою нейтраллю і напругою 220 В, частотою 50 Гц. Згідно з НПАОП 40.1-1.21-98 приміщення можна віднести до категорії без підвищеної небезпеки, оскільки в приміщенні відсутні чинники, що спричиняють підвищену або особливу небезпеку

Для створення безпечних умов праці необхідно провести низку організаційних і технічних заходів. Згідно з НПАОП 40.1-1.32-01 для запобігання ураження людини електричним струмом у приміщенні застосовується система занулення.

4.3 Виробнича санітарія у приміщенні

Робота оператора ПК за енерговитратами належить до категорії легких робіт. У таблиці 4.1 наведені оптимальні параметри мікроклімату в приміщеннях, де виконуються роботи операторського типу [20].

Таблиця 4.1 – Параметри мікроклімату для приміщень з ПК

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	22 – 24 °С; 40 – 60 %; до 0,1 м/с
Теплий	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	23 – 25 °С; 40 – 60 %; 0,1 – 0,2 м/с

Виміряні за допомогою приладів температура та вологість у лабораторії відповідають вказаним у таблиці для теплого періоду року. Слід зазначити, що для нормалізації параметрів мікроклімату слід використовувати у приміщеннях кондиціювання повітря, або забезпечити подачу свіжого повітря системами вентиляції.

Лабораторія, де виконується робота, має наступні характеристики:

– площа приміщення – 48 м^2 (8 м × 6 м);

– висота – 3,5 м;

– кількість робочих місць – 6 шт.;

– обладнання – стіл з ПК і периферією – 6 шт.

Приміщення, відповідно до ДНАОП 0.00-1.31-99, має забезпечувати 6 м^2 площі та 20 м^3 об’єму на одне окреме робоче місце з ПК [20]. Площа приміщення 48 м^2 та об’єм 168 м^3, на кожне робоче місце приходится 8 м^2 площі і об’єм 28 м^3, тобто вимога виконана.

Приміщення з ПК повинні мати природне та штучне освітлення відповідно до ДБН В.25-28-2006 «Природне і штучне освітлення». Природне світло повинно проникати через бічні світлові прорізи, зорієнтовані, як правило, на північ або північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1.5 %.

Рівень загального штучного освітлення приміщення можна перевірити за допомогою методу питомої потужності, викладеної в [20].

Обчислювальна формула методу:

$$W = \frac{W_{\Sigma}}{S}, \tag{4.1}$$

де W – питома потужність, Вт/м^2;

S – площа приміщення, м^2;

W_{Σ} – загальна потужність освітлювальної установки Вт, яка розраховується за формулою:

$$W_{\Sigma} = W_{св} \cdot n_{св}, \tag{4.2}$$

де $W_{св}$ – потужність одного світильника, Вт;

$n_{св}$ – кількість світильників у приміщенні.

$$W_{\Sigma} = 100 \cdot 4 = 400 \text{ Вт}, \tag{4.3}$$

$$W = \frac{400}{48} = 8{,}33 \text{ Вт/м}^2. \tag{4.4}$$

Питомої потужності 8.33 Вт/м^2 за таблицею Б.3 із [20] відповідає освітленість в 250 лк при мінімальній допустимої освітленості 300 лк.

Отже, для створення сприятливих зорових умов у лабораторії необхідно збільшити кількість світильників або замінити лампи в світильниках на більш потужні.

4.4 Пожежна безпека приміщення

Пожежна безпека – стан об'єкта, при якому виключається можливість пожежі, а у випадку її виникнення запобігає впливу на людей небезпечних чинників пожежі й забезпечується захист матеріальних цінностей.

Пожежна безпека забезпечується системою запобігання пожежі й системою пожежного захисту. У всіх службових приміщеннях обов'язково повинен бути «План евакуації людей при пожежі», що регламентує дії персоналу у випадку виникнення вогнища загоряння, що й указує місця розташування пожежної техніки.

Горючими компонентами у виробничому приміщенні є: перегородки, двері, підлоги, ізоляція кабелів і ін.

Протипожежний захист – це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження його поширення, а також на створення умов для успішного гасіння пожежі.

Джерелами запалювання у виробничому приміщені можуть бути електронні схеми від ПК, прилади, застосовувані для технічного обслуговування, пристрою електроживлення, кондиціювання повітря, де в результаті різних порушень утворюються перегріті елементи, електричні іскри й дуги, здатні викликати загоряння горючих матеріалів.

У сучасних ПК дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні

проведення, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відводу надлишкової теплоти від ПК служать системи вентиляції й кондиціювання повітря. При постійній дії ці системи являють собою додаткову пожежну небезпеку.

Енергопостачання виробничого приміщення здійснюється за допомогою трансформаторної станції та за допомогою двигун-генераторних агрегатів. На трансформаторних підстанціях особливу небезпеку представляють трансформатори з масляним охолодженням. Зважаючи на це перевагу слід віддавати сухим трансформаторам.

ВИСНОВКИ

Для досягнення мети кваліфікаційної роботи були розглянуті різні види біометричних даних і принципи їхньої реалізації. Опрацьовані та проаналізовані вже існуючі методи розпізнавання облич. На основі аналізу предметної області сформульовано постановку задачі і розроблено програмний засіб, який реалізує один із алгоритмів розпізнавання обличчя. Подальший розвиток отримав метод ідентифікації особи за ознаками обличчя.

Для розроблення програмного засобу використано середовище розробки Microsoft Visual Studio 2017 і мову програмування C++, а також додаткову бібліотеку OpenCV – бібліотеку для оброблення зображень алгоритмами комп'ютерного зору.

Розроблено консольний застосунок, під час роботи якого можна навчити каскад декількома методами та побачити результат застосування цих методів. Для навчання було підготовлено базу зображень (4214 негативних і 1813 позитивних). Навчання тривало близько 18 годин. Розпізнавання було виконано приблизно у 84 % випадків. Для підвищення надійності та стабільності програми рекомендується збільшити базу зображень і зробити її різноманітнішою.

За результатами розробленої роботи програми можна зробити такі висновки:

– алгоритми навчання та розпізнавання реалізовані успішно;

– програма з високою ймовірністю розпізнає задане під час навчання обличчя;

– для стабільної роботи програми в домашніх умовах буде достатньо використаної під час проведення експерименту кількості позитивних і негативних зображень.

Область застосування даної програми досить велика. Вона може використовуватися для здійснення контролю доступу до інформації, для

охоронної, наглядової і правоохоронної діяльності. Встановити її можна як на домашній ПК, так і на потужні промислові обчислювальні центри.

Під час виконання розділу «Охорона праці» були визначені небезпечні та шкідливі виробничі чинники. Таким чином, були розроблені заходи і технічні засоби щодо забезпечення безпеки праці працюючого персоналу. Застосування цих заходів дозволить максимально знизити ймовірність отримання травм під час роботи, а також поліпшити умови роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні вказівки з підготовки та захисту кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка, освітньо-професійних програм: «Комп'ютерно-інтегровані технологічні процеси і виробництва», «Комп'ютеризовані та робототехнічні системи» / Упоряд. І. Ш. Невлюдов, Р. В. Артюх, В. В. Безкоровайний, Н. П. Демська, В. В. Євсєєв, О. І. Филипенко, О. М. Цимбал. Харків: ХНУРЕ, 2024. 57 с.

2. Навчальний посібник з підготовки кваліфікаційної роботи бакалавра для здобувачів вищої освіти денної і заочної форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» : Навчальний посібник / І. Ш. Невлюдов, В.А. Андрусевич, О. В. Токарєва, С. П. Новоселов, О. В. Сичова. – Харків : Видавництво Іванченка І. С., 2022. 151 с.

3. ДСТУ 3008:2015 Інформація та документація «Звіти у сфері науки і техніки». Структура та правила офомрлювання. / В. Земцева; Ю. Поліщук, канд. фіз.-мат. наук; Р. Санченко, канд. техн. наук; Л. Шрамко; А. Ямчук (науковий керівник) ДП «УкрНДНЦ» від 22 червня 2015р. № 61 з 2017-07-01.

4. Положення про кваліфікаційну роботу здобувача вищої освіти на другому (магістерському) рівні [Електронний ресурс] : Наказ ХНУРЕ від 06 травня 2021 р. No 143. – Режим доступу: https://nure.ua/wpcontent/uploads/Main_Docs_NURE/143-vid-06.05.2021-pro-vvedennja-v-dijurishennja-vchenoi-radi-universitetu.pdf.

5. Nesterenko V., Allakhveranov R. Face recognition technology: advantages and disadvantages // XII International scientific and practical conference "Global science: prospects and innovations" – Cognum Publishing House, Liverpool, United Kingdom. 2024. pp. 46-49, ISBN 978-92-9472-196-

6. Viacheslav Nesterenko, Rauf Allakhveranov / Automated Methods of Face Recognition / X International Scientific and Practical Conference «Modern problems of science, education and society» – Kyiv, Ukraine.: 2023. pp. 361-364.

7. Основи наукових досліджень : підручник / І. Ш. Невлюдов, Ю. М. Олександров, А. О. Андрусевич, О. О. Чала ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Prague : OKTAN PRINT, 2024. – 468 с.

8. Невлюдов І. Ш. Виробничі процеси та обладнання об’єктів автоматизації: Підручник для студентів вищих навчальних закладів / І. Ш. Невлюдов. – Кривий Ріг: Криворізький коледж НАУ, 2017р. – 444 с.

9. Невлюдов І.Ш. Технічні засоби автоматизації: Підручник / І.Ш. Невлюдов, А.О. Андрусевич, О.І. Филипенко, Н.П. Демська, С.П. Новоселов. – Кривий Ріг : Криворізький коледж НАУ, 2019. – 366 с.

10. Невлюдов І.Ш. Людино-машинний інтерфейс в технічних засобах автоматизації: Навчальний посібник / І.Ш. Невлюдов, О.І. Филипенко, Б.О. Шостак. – Харків : «ХТМТ», 2019. – 244 с.

11. Neil Selwyn, Mark Andrejevic, Chris O’Neill, Xin Gu, Gavin Smith. Facial Recognition Technology in Context / Published online by Cambridge University Press: 28 March 2024, pp. 11 – 28.

12. M. I. Zarkasyi, M. R. Hidayatullah, E. M. Zamzami. Implementation of Facial Recognition in Society / Journal of Physics: Conference Series, Volume 1566, 4th International Conference on Computing and Applied Informatics 2019 (ICCAI 2019) 26-27 November 2019, Medan, Indonesia, pp. 1-5.

13. T. Ahonen, A. Hadid, M. Pietikainen. Face recognition with local binary patterns. Electronic source: https://www.researchgate.net/publication/221304831_Face_Recognition_with_Local_Binary_Patterns, (accessed: 30.09/2024).

14. D. Davis. Facial recognition technology threatens to end all individual privacy, The Guardian, 20-Sep-2019. ICCAI 2019 Journal of Physics: Conference Series 1566 (2020) 012069 IOP Publishing, doi:10.1088/1742-6596/1566/1/0120695

15. Facial Recognition Technology: веб-сайт. URL: https://global.canon/en/technology/facial-recognition2022.html (дата звернення: 13.10/2024).

16. D. Voth. Face recognition technology / IEEE Intell. Syst., vol. 18, no. 3, hlm. 4-7, Mei 2013.

17. Sikender Mohsienuddin, Mustafa Shuaieb Sabri. Facial Recognition Technology / International journal of innovation in engeneering research and technology, Electronic Journal, June 2020, 7(6), pp. 176-184.

18. Гэри Брадскі. Learning OpenCV. Computer Vision with the OpenCV Library / підруч. / Гэри Брадскі, Адріан Кехлер; – O'Reilly Media, 2018. – 580 с.

19. Purbandini, “The comparison of laplacianfaces qr decomposition and linear discriminant analysis qr decomposition algorithm for face recognition system on orthogonal subspace,” J. Teknol., vol. 71, no. 1, pp. 43-47, 2014.

20. Комплекс навчально-методичного забезпечення навчальної дисципліни "Організація керування умовами праці" підготовки освітнього рівня бакалавр усіх спеціальностей та усіх напрямів університету [Електронний ресурс] / ХНУРЕ; розроб.: Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк. – Харків, 2017. – 108 с.