

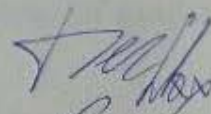
Факультет «Комп'ютерні технології і системи»
Кафедра «Комп'ютерні інформаційні технології»

Пояснювальна записка
до кваліфікаційної роботи магістра

на тему: «Дослідження методів та засобів аутентифікації користувача у реальному часі шляхом розпізнавання обличчя»

за освітньою програмою: 121 Інженерія програмного забезпечення
зі спеціальності: 121 Інженерія програмного забезпечення

Виконав: студент групи ПЗ2221



/Максим РІЗНИЧЕНКО/

Керівник:



/Олександра ГОРБОВА/

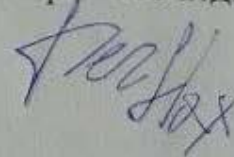
Нормоконтролер:



/Світлана ВОЛКОВА/

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент



Дніпро – 2024 рік

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: «Комп'ютерні технології і системи»
Кафедра: «Комп'ютерні інформаційні технології»
Рівень вищої освіти: магістр
Освітня програма: «Інженерія програмного забезпечення»
Спеціальність: «121 Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри КІТ
_____/Вадим ГОРЯЧКІН/
(підпис)
Дата _____

З А В Д А Н Н Я

на кваліфікаційну роботу для здобуття ступеня магістра
студенту Різниченку Максиму Олександровичу

1. Тема роботи: «Дослідження методів та засобів аутентифікації користувача у реальному часі шляхом розпізнавання обличчя»

Керівник роботи: Горбова Олександра Вікторівна, доцент
затверджені наказом № 1196 ст від 05.12.2022

2. Строк подання студентом роботи: 23.01.2024 р.

3. Вихідні дані до роботи: _____

4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):

4.1 Аналітична частина: аналіз літературних джерел, огляд відомих програмних аналогів, методи виявлення обличчя, методи визначення унікальних характеристик обличчя.

4.2 Обґрунтування загальної методики проведення наукового дослідження: обґрунтування вибору напрямку дослідження, метрики оцінки ефективності, етапи експериментів, розробка тестових сценаріїв, підтримка функціональності.

4.3 Розробка інструментальних засобів для проведення дослідження: зовнішнє проектування, внутрішнє проектування, обґрунтування вибору мови програмування, тестування

4.4 Дослідження ефективності алгоритмів бібліотек для розпізнавання обличчя: результати експериментів, аналіз результатів експериментів.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): діаграма прецедентів, схема взаємодії зон керування системи ескізи екранів, діаграма діяльності, блок-схеми, гістограми.

6. Перелік демонстраційного матеріалу: презентація, демонстраційне відео.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Вступ	20.07.2023-02.08.2023	
2	Аналіз сучасного стану дослідження	02.08.2023-18.09.2023	
3	Обґрунтування загальної методики проведення наукового дослідження	18.09.2023-25.10.2023	
4	Розробка інструментальних засобів для проведення дослідження ефективності алгоритмів бібліотек розпізнавання обличчя	25.10.2023-05.11.2023	30%
5	Дослідження ефективності алгоритмів бібліотек розпізнавання обличчя	05.11.2023-15.11.2023	
6	Аналіз результатів та оформлення пояснювальної записки	15.11.2023-10.12.2023	60%
7	Оформлення тез доповідей	10.12.2023-13.12.2023	
8	Розробка демонстраційних матеріалів	13.12.2023-20.12.2023	100%
9	Подання кваліфікаційної роботи до кафедри	11.01.2024	
10	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.01.2024	

Студент

_____ (підпис)

Максим РІЗНИЧЕНКО

_____ (Ім'я ПРІЗВИЩЕ)

Керівник роботи

_____ (підпис)

Олександра ГОРБОВА

_____ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи магістра складається з вступу, переліку умовних познач, символів, скорочень і термінів, 4 розділів, загальних висновків та рекомендацій, списку використаної літератури:

- вступ. Складається з 1 сторінки;
- розділ 1 аналіз сучасного стану дослідження. Складається з 13 сторінок;
- розділ 2 обґрунтування загальної методики проведення наукового дослідження. Складається з 8 сторінок;
- розділ 3 розробка інструментальних засобів для дослідження ефективності алгоритмів бібліотек розпізнавання обличчя. Складається з 23 сторінок;
- розділ 4 дослідження ефективності алгоритмів бібліотек для розпізнавання обличчя. Складається з 18 сторінок;
- загальні висновки та рекомендації. Складається з 1 сторінки;
- список літератури. Складає 2 сторінки;
- додатки – містить текст програми.

Кількість таблиць: 13 штук.

Кількість рисунків: 45 штук.

Кількість джерел: 16 штук.

Об'єктом цього дослідження є розроблена система авторизації користувача у режимі реального часу з використанням бібліотек розпізнавання обличчя MTCNN та Face-recognition.

Метою роботи є аналіз та оцінка ефективності алгоритмів розпізнавання обличчя бібліотек MTCNN та Face-recognition.

Методи дослідження: імітаційне моделювання процесів аутентифікації шляхом розпізнавання обличчя у режимі реального часу та аналіз статистичних даних виявлених у процесі моделювання.

Результати та їх новизна: результатом роботи є оцінка ефективності алгоритмів розпізнавання обличчя у режимі реального часу бібліотек MTCNN та Face-recognition.

Новизна роботи полягає у чіткому визначенні найбільш ефективного алгоритму розпізнавання обличчя при зміні факторів зовнішнього середовища, які найбільш негативно впливають на процес аутентифікації користувача у режимі реального часу під час використання алгоритмів бібліотек MTCNN та Face-recognition і, як наслідок, набуття подальшого розвитку у цій сфері. Рівень новизни – доповнення.

Ключові слова: СИСТЕМА РЕАЛЬНОГО ЧАСУ, РОЗПІЗНАВАННЯ ОБЛИЧЧЯ, ІДЕНТИФІКАЦІЯ ОСОБИСТОСТІ, КЛЮЧОВІ ТОЧКИ ОБЛИЧЧЯ, КАСКАДНІ ЗГОРТКОВІ НЕЙРОМЕРЕЖІ, ГІСТОГРАМА НАПРЯМЛЕНИХ ГРАДІЄНТІВ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАК, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ.....	10
ВСТУП	11
РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ДОСЛІДЖЕННЯ.....	12
1. Аналіз літературних джерел	12
1.2 Огляд відомих програмних аналогів.....	13
1.2.1 Розпізнавання обличчя у продуктах компанії Apple.....	13
1.2.2 Використання біометричної системи розпізнавання обличчя банківських установ в Україні	14
1.2.3 Надання адміністративних послуг в Україні шляхом розпізнавання обличчя	15
1.2.4 Засіб підтвердження особи від компанії Samsung.....	17
1.3 Сфера застосування. Основні негативні фактори та недоліки. Ризики використання технології.....	17
1.4 Методи виявлення обличчя.....	19
1.4.1 Алгоритм Віоли-Джонса. Ознаки Хаара	19
1.4.2 Теплові камери	20
1.4.3 Згортова нейронна мережа CNN	21
1.4.4 Гістограма напрямлених градієнтів	21
1.5 Методи визначення унікальних характеристик обличчя.....	22
1.5.1 Традиційний метод	22

	8
1.5.2 Аналіз текстури шкіри.....	23
Висновки до першого розділу.....	24
РОЗДІЛ 2 ОБГРУНТУВАННЯ ЗАГАЛЬНОЇ МЕТОДИКИ ПРОВЕДЕННЯ НАУКОВОГО ДОСЛІДЖЕННЯ	25
2.1 Обґрунтування вибору напрямку дослідження	25
2.2 Метрики оцінки ефективності	27
2.2.1 Точність виявлення обличчя.....	27
2.2.2 Час виявлення обличчя.....	27
2.2.3 Ресурсоемність	27
2.2.4 Матриця помилок.....	28
2.2.5 F-міра(F-Score).....	28
2.2.6 Стійкість до змін умов навколишнього середовища.....	30
2.3 Етапи експериментів. Розробка тестових сценаріїв	30
2.4 Підтримка функціональності	31
Висновки до другого розділу	32
РОЗДІЛ 3 РОЗРОБКА ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ДЛЯ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ БІБЛІОТЕК РОЗПІЗНАВАННЯ ОБЛИЧЧЯ	33
3.1 Зовнішнє проектування	33
3.1.1 Функціональне призначення.....	33
3.1.2 Експлуатаційне призначення	33
3.1.3 Функціональні вимоги.....	33
3.1.4 Вхідні дані.....	34
3.1.4 Вихідні дані.....	34

	9
3.1.5 Опис зовнішнього інформаційного середовища.....	34
3.2 Внутрішнє проектування.....	35
3.2.1 Статична архітектура системи, моделювання залежностей	35
3.2.2 Структура внутрішнього сховища даних	36
3.2.3 Особливості інтерфейсу користувача	37
3.2.4 Моделювання процесу виконання операцій	41
3.3 Обґрунтування вибору мови програмування Python	42
3.4 Тестування	43
3.4.1 Тестування білою скринькою	43
3.4.2 Тестування чорною скринькою	46
3.4.3 Налагодження програми.....	54
Висновки до третього розділу.....	56
РОЗДІЛ 4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ БІБЛІОТЕК ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ	57
4.1 Результати експериментів.....	57
4.2 Аналіз результатів експериментів	70
Висновки до четвертого розділу.....	74
ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	77
ДОДАТКИ.....	80

ПЕРЕЛІК УМОВНИХ ПОЗНАК, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС – операційна система

ПЗ – програмне забезпечення

МТСNN(Multi-Task Cascaded Convolutional Networks) – багатозадачна каскадна згорткова нейромережа.

HOG(Histogram of Oriented Gradients) – гістограма напрямлених градієнтів

API – інтерфейс програмування застосунків

Детектор ключових точок – алгоритм для визначення положення ключових точок (очей, носа, рота) на зображенні обличчя

ВСТУП

Сучасні аналітичні системи розпізнавання обличчя щодня застосовуються для збору статистичної інформації, яку емоційне обличчя людини здатне відтворювати щохвилини. Зокрема, широкого розповсюдження набувають системи ідентифікації особи у режимі реального часу. Такі системи досить добре працюють за ідеальних умов, але можуть з легкістю зазнавати втрат у часі або якості при мінімальній зміні навколишнього середовища. Саме тому актуальною залишається проблема швидкості та якості роботи систем розпізнавання обличчя при зміні освітлення, наявності перешкод на обличчі людини, позиції людини у кадрі. Розвиток у цій сфері дозволить ефективніше використовувати системи аутентифікації користувача шляхом розпізнавання обличчя не тільки за оптимальних умов, а й в ситуації наявності негативних факторів, що впливають на процес розпізнавання.

Актуальність та практична цінність роботи полягає у чіткому визначенні найбільш ефективного алгоритму розпізнавання обличчя при зміні факторів зовнішнього середовища, які найбільш негативно впливають на процес аутентифікації користувача у режимі реального часу під час використання алгоритмів бібліотек MTCNN та Face-recognition, що дозволить ефективніше використовувати алгоритми бібліотек не тільки за оптимальних умов, а й в ситуації наявності негативних факторів, що впливають на процес розпізнавання.

Основні положення магістерської роботи доповідалися та були схвалені на XVII міжнародній науково-практичній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» (Дніпро, УДУНТ, 13-14 грудня 2023 року) і на семінарах кафедри КІТ впродовж жовтня-листопада 2023 року.

Публікації за темою роботи. За результатами роботи опубліковано тези доповідей на міжнародній науковій конференції[1].

РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ДОСЛІДЖЕННЯ

1. Аналіз літературних джерел

Для будь-якого дослідження досить важливо проаналізувати існуючі літературні джерела, адже вони допомагають зрозуміти тенденції, досягнення та напрями розвитку у розглянутій сфері.

Комп'ютерний зір є частиною галузі комп'ютерних наук, який потрібен для розуміння інформації з цифрових зображень або відео. Існує величезна кількість завдань, які виконує комп'ютерний зір за допомогою використання методів створення числових або символічних представлень інформації, яка була отримана з реального світу. Одним з них є виявлення та розпізнавання обличчя людей. Наступними кроками є обробка, аналіз та розуміння цифрових зображень, трансформація образів у інформацію, яку може зрозуміти комп'ютер. Зображення можна розглядати як символічну або числову інформацію за допомогою моделей побудованих з використанням законів геометрії, фізики, статистики та машинного навчання.[2]

Розпізнавання обличчя – техніка, яка ідентифікує людське обличчя на цифровому зображенні. Розпізнавання обличчя є відносно зрілою технологією, проте вона все ще потребує вдосконалення. Один із найпоширеніших методів розпізнавання обличчя – це метод виявлення обличчя Віоли-Джонса, широко відомий як каскади Хаара. Каскади Хаара були винайдені задовго до того, як глибоке навчання стало популярним і є одним із найбільш часто використовуваних методів виявлення облич.

У літературі широко розглядають різні технології та методи розпізнавання обличчя. Деякі з основних підходів включають в себе використання глибоких нейронних мереж, каскадних класифікаторів та технік попередньої обробки зображень. Роботи таких авторів як Голуб'як І. В, Косаревич Р. Я.[3], Тимошин Ю. А., Орленко С. П.[4], Р. Viola and M.J. Jones[5] висвітлюють переваги та недоліки цих підходів.

Більшість існуючих методів розпізнавання обличчя ефективно працюють на фронтальних обличчях і здатні досягти низького рівня помилок у добре

контрольованому середовищі. Однак, огляд літератури показав, що зміна пози або ж факторів навколишнього середовища є важливою невирішеною проблемою при розробці системи автоматичного розпізнавання обличчя в реальному часі. Труднощі з розпізнаванням обличчя в різних позах та умовах освітлення пов'язані з тим фактором, що дисперсія в межах класу домінує між класовим розкидом даних і призводить до втрати дискримінаційних даних ознак. До того ж, великою проблемою є конфіденційність та безпека даних при використанні технологій розпізнавання.

1.2 Огляд відомих програмних аналогів

1.2.1 Розпізнавання обличчя у продуктах компанії Apple

У 2017 році компанія Apple представила новий продукт, який дозволив би підвищити безпеку, так званий FaceID. Біометрична інформація, а саме математичний образ відсканованого обличчя, користувача зберігається всередині процесора. Таким чином, інформація знаходиться у повній безпеці і не може бути нікуди надіслана. Сам сенсор складається з двох модулів: перший – відображає ключові точки на обличчі користувача, другий – перевіряє шаблон з наявним всередині процесора.

FaceID за допомогою нейронних мереж самонавчається і адаптується до змін навколишнього середовища. Добре працює в тепряві, з головними уборами, окулярами, макіяжем на обличчі користувача.

Система використовується для сплати товарів, аутентифікації користувача, розблокування додатків та у банківських сервісах. Етапи роботи системи FaceID зображені на рисунку 1.1:

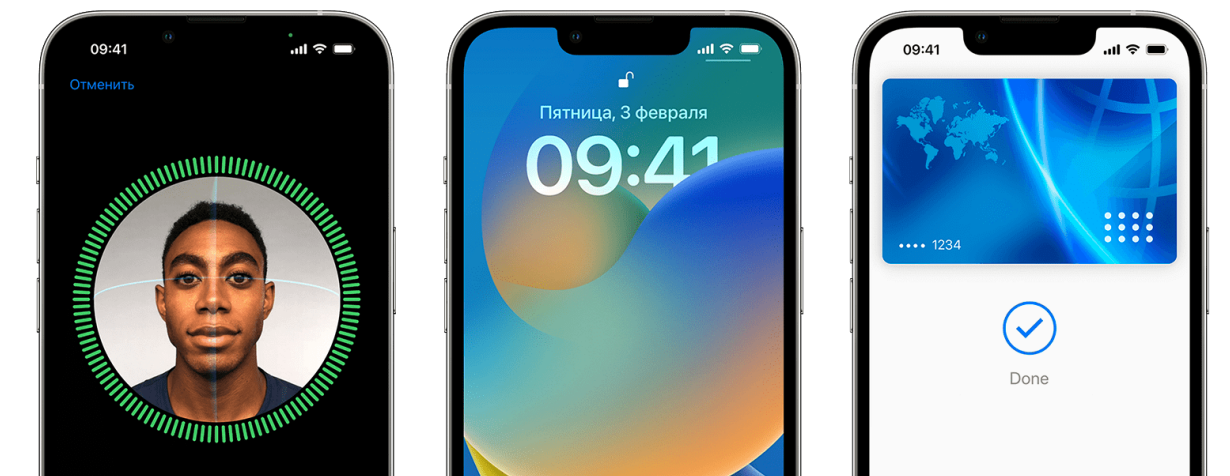


Рисунок 1.1 – Етапи роботи системи FaceID

Основні недоліки системи полягають в тому, що спрацювання відбувається досить довго. Потрібно вмикнути дисплей, піднести пристрій до лица та чекати відповіді. До того ж, для стабільної роботи необхідно, щоб користувач розташовувався вертикально до пристрою з відкритими очима, інакше система не спрацює. Система працює лише на продукції компанії Apple.

1.2.2 Використання біометричної системи розпізнавання обличчя банківських установ в Україні

Технологія оплати товарів шляхом розпізнавання обличчя клієнтом реалізована ПриваБанком та Visa. Технологія не потребує банківської карти або смартфона у клієнта. Для реєстрації додаток Приват24 запрошує у клієнта три фото прямий ракурс, під кутом 45 градусів вліво та вправо. Після реєстрації клієнт може спокійно зайти, наприклад, до кав'ярні, яка має у наявності термінал з камерою та оплатити свій товар просто за допомогою обличчя[6].

Створена на ядрі від Amazon Rekognition та AWS Lambda, FacePay24 – відносно нова технологія, проте користувачі активно реєструють свої біометричні дані у додатку та користуються нею у повсякденному житті. Процес сплати обличчям системи FacePay24 зображений на рисунку 1.2:

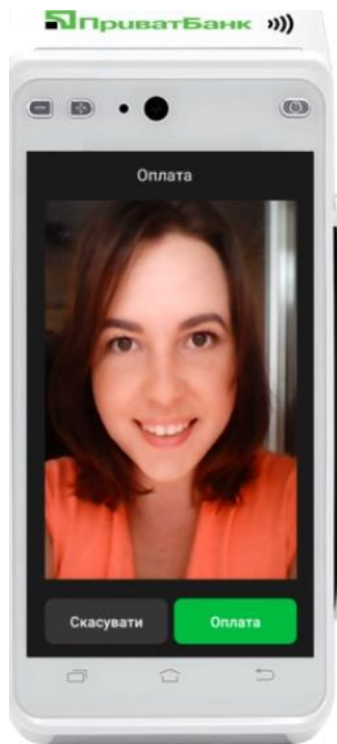


Рисунок 1.2 – Процес оплати обличчям системи FacePay24

Не зважаючи на усі переваги технології, вона має і недоліки. Систему все ще можливо обійти в деяких випадках. Систему тестували на близнюках і там вона помиляється, бо моделі розпізнавання ще не відрізняють мікроелементи. У близнюків відстань ключових точок майже ідентична, саме тому надійність системи залишається під запитанням. До того ж, система працює лише у певних мережах торгових точок та ще не впроваджена всюди.

1.2.3 Надання адміністративних послуг в Україні шляхом розпізнавання обличчя

Міністерство цифрової трансформації України використовує біометричні дані громадянина України для ідентифікації у додатку «Дія». Алгоритми системи зводяться до зіставлення або вимірювання відстані між визначеними ключовими точками на обличчі. Орієнтири використовуються для масштабування та вирівнювання обличчя для більш точного порівняння та розпізнавання. Незалежно від розташування обличчя, можна відцентрувати очі та рот на зображенні приблизно в однаковому положенні, що зробить наступне зіставлення більш точнішим. Візуальний макет процесу визначення ключових точок зображень на рисунку 1.3:

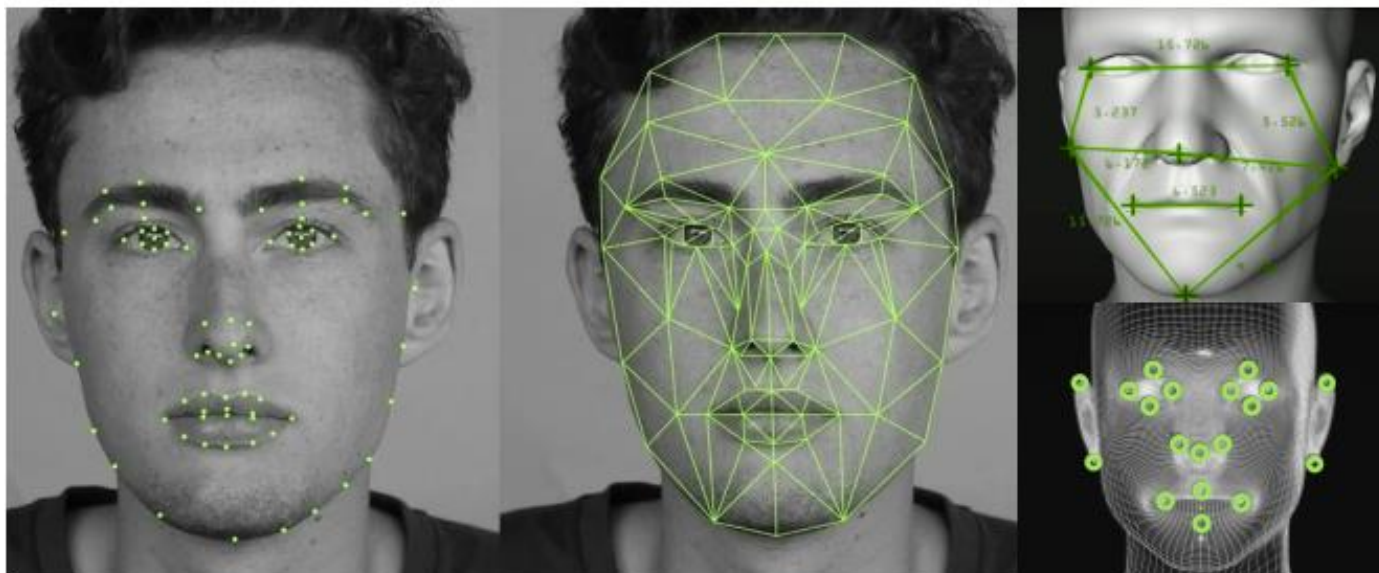


Рисунок 1.3 – Візуальний макет процесу визначення ключових точок

При зіставленні носа враховуються його розмір та форма, при зіставленні в області рота береться до уваги форма губ та відстань між нижньою частиною носа та верхньою губою. Нижня частина обличчя характеризується формою підборіддя.

Зіставлення особи проводиться з урахуванням наявності шрамів, що перекривають контрольні точки. При цьому потрібно взяти до уваги додаткові антропометричні точки[7]. До того ж, точки на обличчі не повинні закриватися зайвими предметами, особливо волоссям. Класифікація підборіддя при розпізнаванні зображена на рисунку 1.4:



Рисунок 1.4 – Класифікація підборіддя при розпізнаванні

1.2.4 Засіб підтвердження особи від компанії Samsung

Інженери компанії Samsung також створили власний аналог FaceID під назвою Samsung Face Recognition, який використовується для підтвердження особи на пристроях компанії. Під час розпізнавання використовується зображення з фронтальної камери, сканується обличчя людини, проводиться аналіз на відповідність з даними, що наявні у системі. Біометрична інформація користувача охороняється спеціальною системою Кнох, що дозволяє захистити їх на рівні системи. Процес авторизації користувача у системі Samsung Face Recognition зображений на рисунку 1.5:

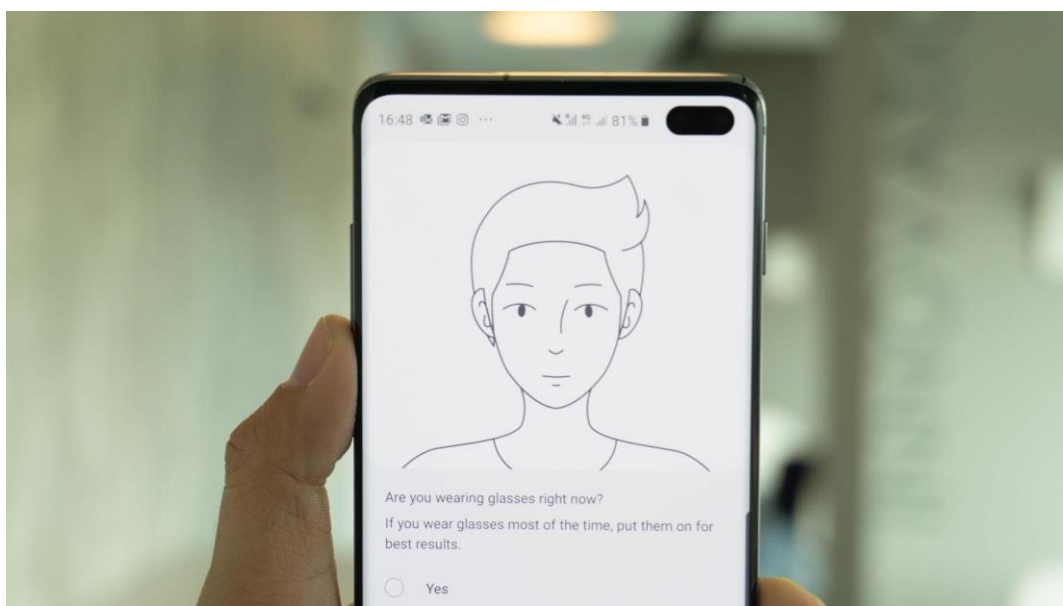


Рисунок 1.5 – процес авторизації користувача у системі Samsung Face Recognition

Samsung Face Recognition була створена та націлена на прототип використання, саме тому система поступається надійністю. Часті хибні розпізнавання, великі проблеми при розпізнаванні у погано освітленому навколишньому середовищі, закрита система для продукції компанії Samsung.

1.3 Сфера застосування. Основні негативні фактори та недоліки. Ризики використання технології

Області застосування систем розпізнавання обличчя досить широкі. Використання подібних систем вже впроваджено, наприклад, для верифікації клієнтів

фінансових установ та банків, онлайн-страхування, здійснення покупок, безконтактної ідентифікації в логістиці, контролю та автоматизації якості виробництва, надання адміністративних послуг, авторизації на пристроях, збору статистичної інформації, безпекової діяльності.

Технології комп'ютерного зору використовуються у системах вуличного відеоспостереження. Прикордонники за допомогою американської системи розпізнавання облич Clearview AI[8] встановили понад десяти тисяч осіб, які брали участь у російських воєнних злочинах. Серед них ті, хто незаконно переправляв дітей, військовослужбовці, колаборанти, зрадники.

Київська обласна військова адміністрація впровадила систему розпізнавання облич «Безпечна Київщина». Було інтегровано понад 500 камер з функцією розпізнавання обличчя, що значно знизило рівень злочинності та дозволило оперативно розкривати злочини.[9]

Компанія Google створила продукт для відкривання дверей будинку, який працює на базі системи розпізнавання обличчя. Відео з дзвінка у реальному часі передається на пристрій користувача. Вхід до дверей будинку виконується шляхом ідентифікації з раніше завантаженими фото власника.

Існують системи, які працюють на базі процесу розпізнавання обличчя, що дозволяють допомогти людям з аутизмом розуміти соціальні сигнали шляхом вимірювання емоцій людини на зображенні.

Системи розпізнавання обличчя людини досить добре працюють в ідеальних умовах, але при мінімальній зміні, наприклад, кута нахилу голови людини такі системи можуть зазнавати труднощів. Крім цього, існують проблеми з низькою роздільною здатністю зображення, багатою мімікою людини на фото, зміною освітлення на знімку, старіння особи.

Основні ризики використання систем розпізнавання обличчя полягають у високій ймовірності їх зламу чи помилок під час процесу. До того ж існує велика ймовірність потрапляння баз даних із зображеннями людей до злоумисників.

1.4 Методи виявлення обличчя

Процес розпізнавання обличчя поділяється на декілька етапів: виділення облич на кадрі, попередня обробка зображення, визначення унікальних характеристик обличчя, ідентифікація особи. Відокремлення обличчя потребує створення певного набору правил за якими система буде класифікувати певний фрагмент зображення людським обличчям[10].

Загальний алгоритм розпізнавання обличчя представлений на рисунку 1.6:

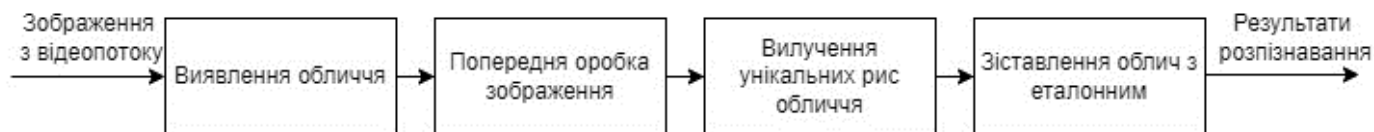


Рисунок 1.6 – Загальний алгоритм розпізнавання обличчя

1.4.1 Алгоритм Віюлі-Джонса. Ознаки Хаара

Кожне обличчя людини має свої характеристики та унікальні риси. Для розпізнавання особи необхідно відокремити основні елементи обличчя. Очі, ніс, губи, лоб присутні на кожному лиці окремої особи. Саме це дозволяє за допомогою певних ознак відокремити область на зображенні, де може знаходитись обличчя людини.

Ознаки Хаара складаються з суміжних прямокутних областей, які розташовуються на зображенні. Потім сумуються інтенсивності пікселів в областях і вираховується різниця між сумами. Така різниця і є значенням конкретного признака, розміра образу на зображенні.

Спільним для усіх облич людей є те, що область навколо очей темніша за область у зоні центру щоки. Ключовою відмінністю областей ознак Хаара є найбільша у порівнянні з іншими ознаками швидкість.

Вигляд примітивів Хаара зображений на рисунку 1.7:

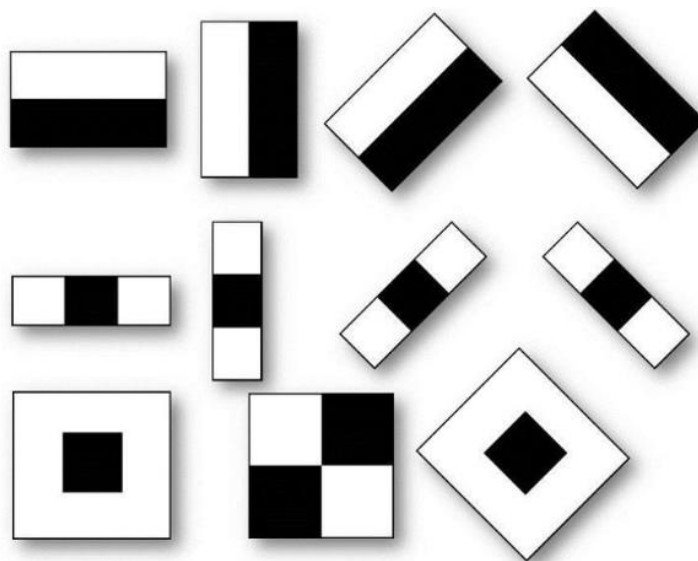


Рисунок 1.7 – Зображення примітивів Хаара

1.4.2 Теплові камери

Одним з ефективних рішень проблеми наявності перешкод на обличчі людини є теплові знімки, які враховують лише форму голови особи. При цьому ігноруються різноманітні аксесуари та головні убори. Теплові камери захоплюють зображення обличчя навіть в умовах слабкого освітлення. Теплове зображення обличчя з камери продемонстроване на рисунку 1.8:

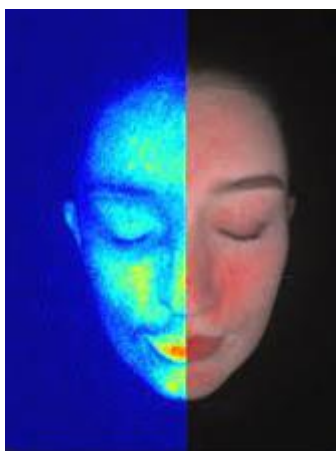


Рисунок 1.8 – Теплове зображення обличчя

Проблема пов'язана з використанням теплових камер полягає в тому, що бази даних для розпізнавання облич обмежені.

1.4.3 Згорткова нейронна мережа CNN

Згорткова нейронна мережа дозволяє виділити опрні ознаки зображення, такі як ребра, контури, грані. Такі ознаки складаються в фрагменти текстур, які далі допомагають визначити об'єкт на зображенні. Результат роботи згорткової нейронної мережі для виявлення обличчя представлений на рисунку 1.9:



Рисунок 1.9 – Робота згорткової нейронної мережі

1.4.4 Гістограма напрямлених градієнтів

За допомогою обчислення значень градієнта та застосуванні одновимірної центрованої дискретної маски похідної у горизонтальному та вертикальному напрямках фільтруються дані кольору зображення. У результаті чого формується зображення контурів об'єкта, що дає змогу у подальшому розпізнати предмет на зображенні. Процедура включає наступні кроки:

- обчислення градієнтів. Зображення перетворюють в чорно-біле та обчислюють горизонтальні та вертикальні градієнти кожного пікселя;
- обчислення амплітуди та напрямку градієнту для кожного пікселя;
- розділення зображення на клітинки та блоки;
- побудова глобальної гістограми.

Результат роботи побудови гістограми напрямлених градієнтів зображень на рисунку 1.10:

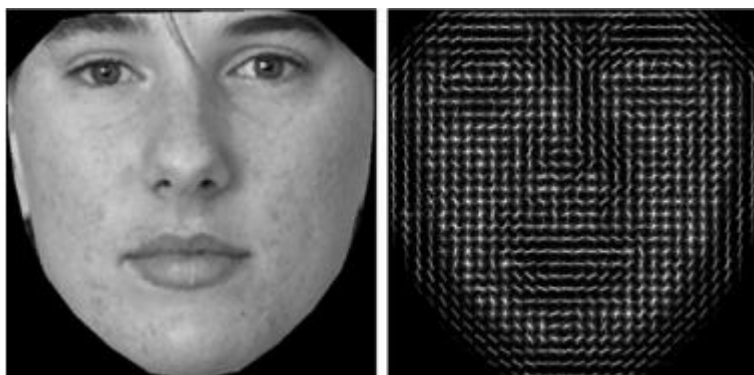


Рисунок 1.10 – Результат роботи побудови гістограми напрямлених градієнтів

1.5 Методи визначення унікальних характеристик обличчя

1.5.1 Традиційний метод

Традиційний метод, або ж геометричний, полягає в тому, щоб закріпити на певному обличчі ключові точки притаманні лише цій особі та підрахувати відносну позицію, розмір, форму окремих ознак лица. Такі підрахунки використовуються для пошуку інших зображень з відповідними характеристиками. Метод потребує високоякісного зображення та надійного алгоритму пошуку ключових точок. При цьому обов'язкове гарне освітлення та невеликий кут нахилу особи на фронтальному зображенні. Вираз обличчя має бути нейтральним. Замість використання складних алгоритмів нейронних мереж, геометричний метод використовує прості математичні правила для виявлення анатомічних особливостей обличчя та їх заємозв'язків. Метод включає наступні кроки:

- локалізація обличчя – визначення регіону, де може знаходитися обличчя, зазвичай проводиться на основі якихось загальних характеристик, таких як розташування очей, носа та рота;
- визначення ключових точок;
- аналіз геометричних відносин – використання геометричних правил для визначення розташування та взаємоположення ключових точок.

Наприклад, можна використовувати відстані та кути між очима, співвідношення розмірів рота відносно очей тощо;

- перевірка геометричних орієнтованих шаблонів – використання шаблонів або моделей для перевірки геометричних особливостей обличчя. Це може включати перевірку певних пропорцій чи відстаней між ключовими точками.

Геометричний метод може бути ефективним у випадках, коли обличчя має стандартні форми та анатомічні відносини, але він може бути менш точним або менш стійким до варіацій у формі та розташуванні обличчя порівняно з більш сучасними методами, такими як глибоке навчання для розпізнавання обличчя

1.5.2 Аналіз текстури шкіри

Використання унікального малюнку шкіри людини також широко використовуваний метод розпізнавання обличчя. Він використовує візуальні деталі шкіри, перетворює унікальні лінії та плями в математичний простір. Система розпізнавання за текстурою шкіри розбиває знімок поверхні на дрібні частини, розрізняються усі лінії, що дозволяє ефективніше використовувати процес ідентифікації.

Результат роботи аналізу текстури шкіри зображений на рисунку 1.11:

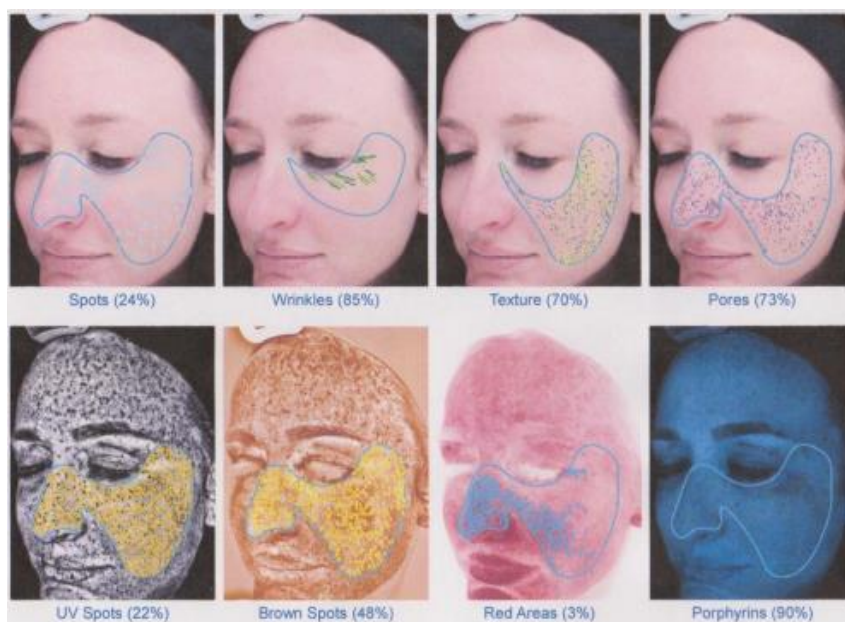


Рисунок 1.11 – Результат роботи аналізу текстури шкіри

Висновки до першого розділу

Проведено ретельний аналіз літературних джерел, розглянуто відомі методи та техніки попередньої обробки зображень, виявлено невирішені проблеми процесу розпізнавання під час зміни навколишнього середовища. Переглянуто вже реалізовані системи та готові рішення серед найпопулярніших аналогів. Визначені основні негативні фактори та ризики у сфері застосування систем розпізнавання обличчя, описано загальний алгоритм розпізнавання обличчя людини, методи виявлення та визначення унікальних характеристик обличчя.

На основі аналізу сучасного стану дослідження були зібрані основні вимоги до систем розпізнавання обличчя, що зображені на рисунку 1.12:

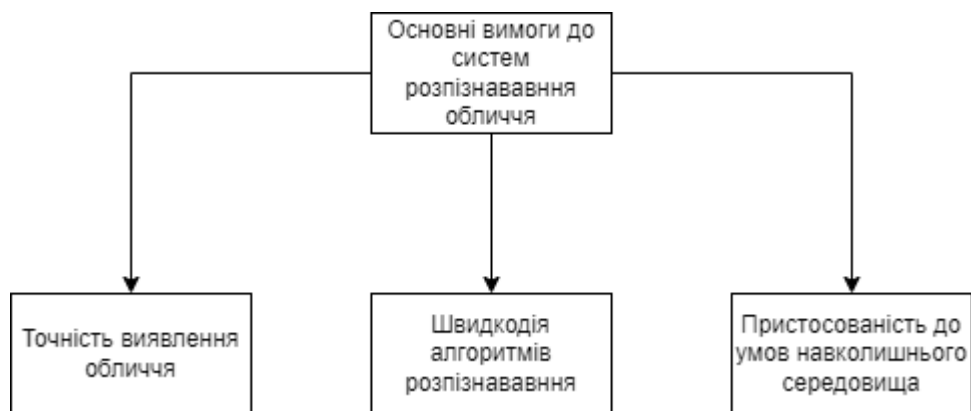


Рисунок 1.12 – Основні вимоги до систем розпізнавання обличчя

Визначені вимоги допоможуть зосередити зусилля проведення наукового дослідження саме на важливих аспектах процесу розпізнавання обличчя.

РОЗДІЛ 2 ОБГРУНТУВАННЯ ЗАГАЛЬНОЇ МЕТОДИКИ ПРОВЕДЕННЯ НАУКОВОГО ДОСЛІДЖЕННЯ

2.1 Обґрунтування вибору напрямку дослідження

Дослідження присвячене основним проблемам та недолікам систем розпізнавання обличчя на основі бібліотек: Face-recognition[11] та MTCNN[12]. Робота націлена на виявлення переваг та недоліків алгоритмів бібліотек при використанні їх у системах авторизації користувача у режимі реального часу шляхом розпізнавання обличчя.

Face-recognition – бібліотека розпізнавання обличчя, що побудована на C++ бібліотеці dlib. Відрізняється високою точністю розпізнавання. Легка у використанні та має досить прості вимоги. Алгоритми виявлення обличчя працюють за допомогою використання гістограми напрямлених градієнтів. Метод рахує напрямки градієнта в частині зображення, де є обличчя людини.

MTCNN – бібліотека багатозадачної каскадної згорткової нейронної мережі, яка працює шляхом створення великої кількості розмірів зображення, розпізнавання обличчя всередині квадрату фіксованого розміру на кожному зображенні. Модель MTCNN адаптована з реалізації MTCNN Facenet на основі трьох основних ключів p-net, r-net та o-net.

P-net – нейронна мережа, яка після створення різних копій зображення використовує певний блок пікселів, який буде сканувати всі копії зображення починаючи з верхнього лівого кута рухаючись на декілька пікселів далі. Після чого, p-net надає координати блоків і їх рівень довіри, яких характеризує наявність обличчя у певному блоці.

R-net – нейронна мережа, яка проводить відбір блоків з найбільшою довірою. На цьому етапі формуються повнозв'язні шари. Вихідні дані r-net досить схожі на вихідні дані p-net.

O-net – нейронна мережа, яка є останньою частиною MTCNN мережі. Вона формує п'ять точок для кожного обличчя, а саме: ніс, очі, кути губ. Якщо точки повністю

потрапляють у блок, то він помічається як блок з найбільшою довірою. В ньому ймовірність зображення обличчя максимальна.

Схема роботи згорткової нейронної мережі вказана на рисунку 2.1:

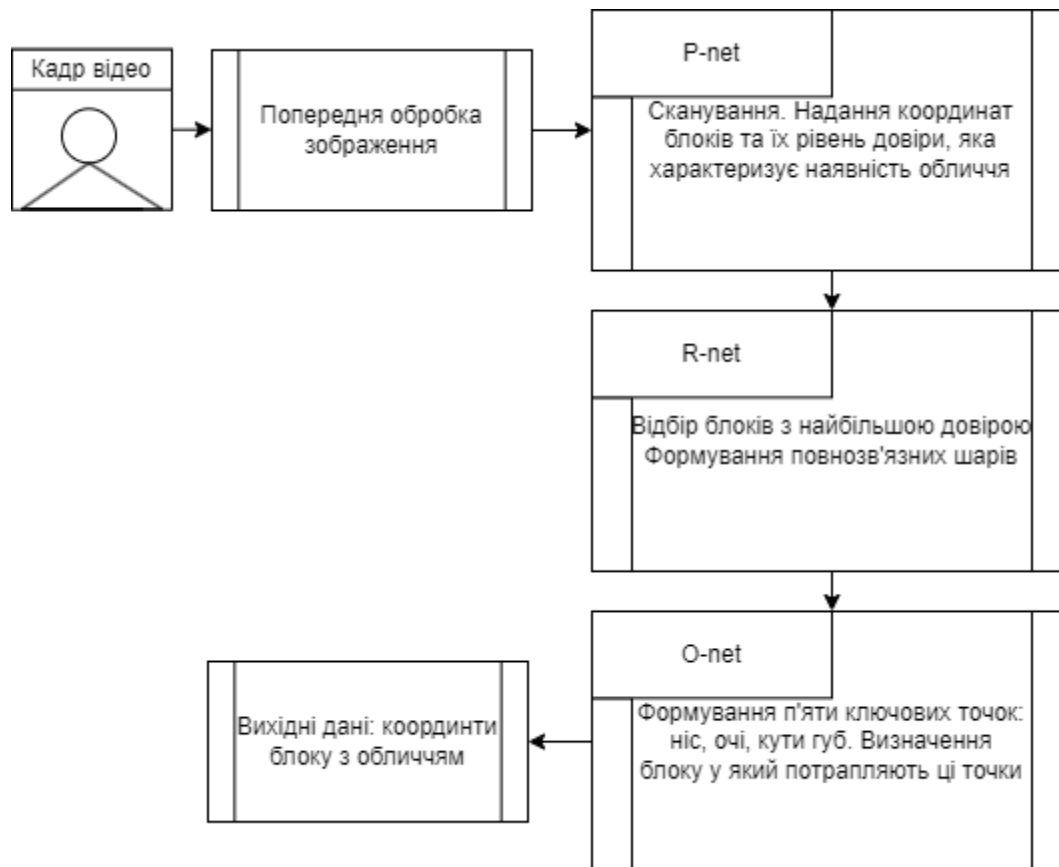


Рисунок 2.1 – Схема роботи згорткової нейронної мережі

Під час дослідження будуть враховуватись фактори роботи існуючих бібліотек розпізнавання обличчя при зміні умов навколишнього середовища. Низький рівень освітлення, зміна кута нахилу обличчя, наявність перешкод на обличчі, зміна дистанції обличчя до камери є особливими факторами, що досить вагомо впливають на результат алгоритмів розпізнавання. Аналізуючи ці аспекти, можна визначити реальну ефективність алгоритмів розпізнавання бібліотек та їх можливості адаптації до різноманітних умов.

Аналіз точності виявлення людського обличчя у кадрі, швидкодії роботи алгоритмів, простоти використання, інтеграції з зовнішніми бібліотеками, складність API, визначення обмежень та недоліків функціоналу бібліотек допоможуть отримати

реалістичну картину того, наскільки ефективно можна використовувати обрану бібліотеку для конкретних завдань.

2.2 Метрики оцінки ефективності

2.2.1 Точність виявлення обличчя

Точність не є кінцевим результатом, адже вона не має інформації про характер помилок, проте досить корисний показник на початку оцінки

$$Accuracy = \frac{\#correct\ answers}{all\ classified\ answers}$$

Точність – це відношення правильно розпізнаних облич до загальної кількості спроб. Точність дозволяє оцінити загальну ефективність алгоритму, але вона може бути неінформативною у разі незбалансованих даних.

2.2.2 Час виявлення обличчя

Часова ефективність алгоритму – характеристика продуктивності алгоритму, що визначається кількістю елементарних операцій, які потрібно виконати для реалізації алгоритму. Оцінка швидкості роботи алгоритму під час пошуку обличчя в режимі реального часу особливо важлива для подібних систем. На відміну від алгоритмів, які можуть виявляти обличчя на статичних зображеннях, реальний час передбачає, що дія буде відбуватися швидко і без затримок, дозволяючи системі працювати в режимі, близькому до миттєвого.

2.2.3 Ресурсоємність

Ресурсоємність – характеристика алгоритму, яка вказує, наскільки інтенсивно він використовує ресурси комп'ютерної системи, такі як центральний процесор(CPU), оперативна пам'ять(RAM).

Ресурсоємність центрального процесору(CPU) визначає, наскільки програма вимагає обчислювальних ресурсів. Деякі завдання можуть використовувати велику кількість процесорного часу.

Ресурсоемність оперативної пам'яті(RAM) показує, наскільки програма вимагає обсягу оперативної пам'яті для ефективної роботи. Наприклад, великі обсяги даних або складні обчислення можуть вимагати більше оперативної пам'яті.

2.2.4 Структура матриці помилок

Confusion matrix або ж матриця помилок надає інформацію про те, де ми допускаємось помилки у вигляді умовної таблиці розподілу, що зображена у таблиці 2.1:

Таблиця 2.1 Матриця помилок

	Асепт	Репет
Репет	Type 1 error (False accept)	Correct (True reject)
Асепт	Correct (True accept)	Type 2 error (False reject)

False асепт – коли фактичним значенням було «ні», модель передбачала «так» (тобто неправильне передбачення = хибно спрацював)

True reject – коли фактичним значенням було «ні», модель передбачала «ні» (тобто правильне передбачення)

True асепт – коли фактичним значенням було «так», модель передбачала «так» (тобто правильне передбачення = правильно спрацював)

False reject – коли фактичне значення було "так", модель передбачала "ні" (тобто неправильне передбачення)

Матриця помилок – це таблиця особливого компонування, що надає можливість наочно зобразити продуктивність алгоритму. Вона дозволяє отримати різні метрики, такі як точність, повнота та влучність, що використовуються для оцінки ефективності моделі класифікації. Ці метрики допомагають зрозуміти, наскільки добре модель працює на різних класах і чи має вона тенденцію до певних видів помилок[13].

2.2.5 F-міра(F-Score)

F-міра – це метрика оцінки ефективності моделі в задачах бінарної класифікації, яку обчислюють через влучність та повноту тесту, де влучність – це відношення правильно класифікованих екземплярів об'єкта(True асепт) до усіх об'єктів, які модель визначила як об'єкти(True асепт та False асепт), а повнота – це відношення правильно

класифікованих екземплярів об'єкта(True ассепт) до усіх реальних об'єктів(True ассепт та False reject). Наочна оцінка F-міри продемонстрована на рисунку 2.2:

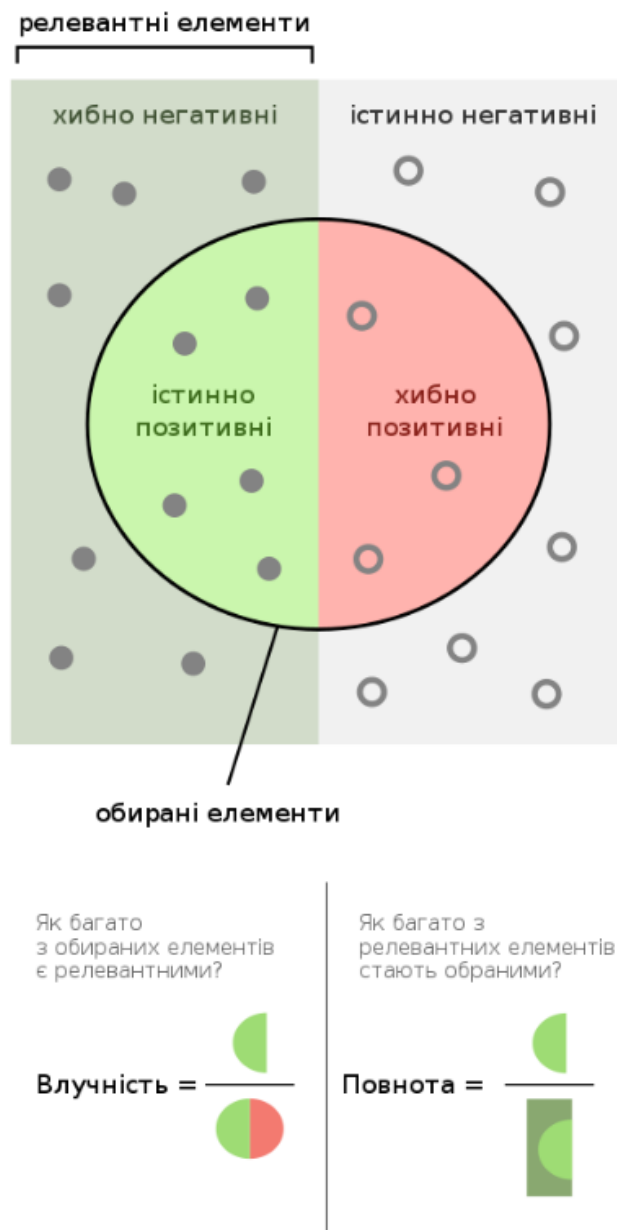


Рисунок 2.2 – Оцінка F-міри

У контексті дослідження ефективності алгоритмів бібліотек розпізнавання обличчя F-міра може бути використана для оцінки системи розпізнавання, зокрема, її здатності точно визначати обличчя і уникати неправильних визначень[14].

2.2.6 Стійкість до змін умов навколишнього середовища

По-перше, великою проблемою процесу розпізнавання обличчя є освітлення. Бібліотека MTCNN використовує каскадні класифікатори для виявлення обличчя, що може покращити результати проходження експерименту високою стійкістю до різних умов освітлення. Методи Face-recognition також здатні працювати при різних рівнях освітлення, але точність може зменшитись при його недостатній кількості.

По-друге, важливою умовою навколишнього середовища під час розпізнавання є поза обличчя під кутом. Бібліотека MTCNN повинна добре працювати з різними позами обличчя під кутом, натомість face-recognition може мати проблеми, якщо кут нахилу буде занадто великим.

До того ж, на процес розпізнавання впливають такі фактори як наявність перешкод на обличчі, зміна дистанції до камери. Методи бібліотеки MTCNN повинні мати високу стійкість до змін у зовнішньому вигляді або наявності перешкод на обличчі, зміні дистанції до камери, однак face-recognition може вимагати додаткового навчання для розпізнавання при значних змінах.

2.3 Етапи експериментів. Розробка тестових сценаріїв

Етапи експериментів будуть проходити у наступних умовах навколишнього середовища:

- робота алгоритмів при низькому рівні освітлення. Розпізнавання обличчя при низькому рівні освітлення може завдати деякі труднощі, оскільки низьке освітлення може призводити до недостатньої видимості та знижки контрастності зображення;
- робота алгоритмів, коли обличчя знаходиться під кутом до камери. Розпізнавання обличчя під кутом до камери може завдати деякі труднощі, оскільки змінюється геометрія обличчя, його проекція та видимість ключових ознак;
- робота алгоритмів при наявності перешкод на обличчі. Алгоритми розпізнавання обличчя можуть стикатися з труднощами, коли на

зображенні присутні перешкоди на обличчі. Ці перешкоди можуть включати окуляри, волосся, маски, часткові перекриття та інші елементи, які можуть ускладнити роботу алгоритмів;

- робота алгоритмів при зміні дистанції до камери. Зміна дистанції до камери може впливати на роботу алгоритмів розпізнавання обличчя. Основні проблеми, пов'язані з цим, включають зміну розмірів обличчя на зображенні та зміну пропорцій між різними частинами обличчя.

2.4 Підтримка функціональності

Бібліотеки MTCNN та Face-recognition мають широкий набір функціональності, яка дозволяє використовувати їх для різноманітних систем розпізнавання обличчя. У таблиці 2.2 наведено загальний огляд порівняння функціональності цих бібліотек:

Таблиця 2.2 Загальний огляд порівняння функціональності бібліотек

	MTCNN	Face-recognition
Виявлення обличчя	Може виявляти обличчя, очі та рот з великою точністю	Може виявляти обличчя та очі в цілому
Визначення ключових точок (landmarks):	Надає можливість визначати ключові точки обличчя, що полегшує аналіз особливостей обличчя	Дозволяє визначати ключові точки обличчя, такі як очі, ніс та рот
Ідентифікація та зіставлення	Не має такого функціоналу	Надає можливість ідентифікувати обличчя та здійснювати зіставлення за зразком, що спрощує визначення осіб на зображеннях
Оцінка Подібності	Не має такого функціоналу	Можливість оцінювати подібність між обличчями на різних зображеннях

Як бачимо, бібліотека Face-recognition серед функціоналу має такі можливості як ідентифікація, зіставлення та оцінка подібності обличчя на зображенні, тож для повної оцінки ефективності алгоритмів цієї бібліотеки потрібно провести експерименти не тільки з визначення обличчя, а й інших функціональних можливостей.

2.5 Методи збору статистичних даних

У якості методу збору статистичних даних було обрано допоміжну бібліотеку для мови python – psutil. Вона є потужним інструментом для моніторингу системних ресурсів та процесів операційної системи, надає простий та зручний інтерфейс для отримання інформації щодо використання центрального процесора, оперативної пам'яті, а також інших параметрів системи.

Psutil забезпечує інформацію про запущені процеси, їхні характеристики та інші деталі, що може бути корисним при вивченні ефективності алгоритмів розпізнавання обличчя на систему. Ця бібліотека відкриває можливості для глибокого аналізу та оптимізації роботи алгоритмів в реальних умовах експлуатації. Таким чином, використання psutil стає важливим елементом методичної бази дослідження, дозволяючи отримувати об'єктивні дані та забезпечуючи докладний моніторинг системи під час експериментів.

Висновки до другого розділу

Детально розглянуто та обґрунтовано стратегію та мету проведення наукового дослідження. Описано основний процес дослідження, етапи експериментів та головні метрики оцінки ефективності алгоритмів розпізнавання обличчя бібліотек MTCNN та Face-recognition. Обрана методологія відображає доцільність та ефективність вирішення існуючої проблеми. Чітко визначені об'єкт та предмет дослідження, обрано конкретні методи, що спроможні надати вичерпні відповіді на представлену проблему. Наявна методика створює надійну основу для проведення дослідження з високим ступенем достовірності та перспективами для подальших вивчень у цій галузі.

РОЗДІЛ 3 РОЗРОБКА ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ДЛЯ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ БІБЛІОТЕК РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

3.1 Зовнішнє проектування

3.1.1 Функціональне призначення

Функціональне призначення — оперативність отримання доступу, ідентифікації та верифікації осіб за допомогою системи авторизації користувача у режимі реального часу шляхом розпізнавання обличчя. Інструментом дослідження роботи є використання бібліотек MTCNN та Face-recognition. До функцій відносяться:

- аутентифікація – система може використовуватися для визначення особи на основі її обличчя та порівняння його зі збереженими даними в базі даних. Це дозволяє контролювати доступ до системи.
- верифікація – система може перевіряти, чи відповідає обличчя особи, яка претендує на доступ, зразку обличчя, зареєстрованому в системі. Це допомагає відтворювати особу на основі її біометричних даних.

3.1.2 Експлуатаційне призначення

Експлуатаційне призначення — підвищення безпеки, скорочення часу для контролю доступу до системи. До експлуатаційного призначення відносяться:

- безпека – система забезпечує доступ до інформації за допомогою перевірки обличчя на унікальні характеристики та риси.
- контроль доступу – використання для ідентифікації та аутентифікації осіб для забезпечення доступу до обмежених зон.

3.1.3 Функціональні вимоги

Програмний продукт має забезпечувати можливості:

- реєстрацію нових користувачів шляхом додавання фото;
- реєстрацію нових користувачів шляхом сканування обличчя у режимі реального часу;

- відповідне відображення інформації про успішний або невдалий процес авторизації;
- аутентифікацію користувача у режимі реального часу шляхом сканування обличчя;
- функціонал виявлення обличчя за допомогою нейронних мереж бібліотекою MTCNN;
- функціонал виявлення обличчя бібліотекою Face-recognition;
- збереження фото користувача у системі.

3.1.4 Вхідні дані

Вхідними даними системи є:

- логін (довжина не більше 19 символів);
- фото співробітника(формат .jpg);
- відеозображення з камери пристрою.

3.1.4 Вихідні дані

Вихідними даними системи є:

- виведення повідомлення про успішний або невдалий процес авторизації;
- відображення детекції обличчя шляхом виділення його у прямокутник на екрані;
- відображення відеопотокового зображення при детекції обличчя;
- виведення використання ресурсів оперативної пам'яті;
- виведення використання ресурсів центрального процесору;
- виведення витраченого часу на виконання розпізнавання.

3.1.5 Опис зовнішнього інформаційного середовища

Параметри для збереження фотознімка вводяться користувачем з клавіатури з відповідним контролем введення. Пошук подібності обличчя у системі відбувається шляхом аналізу внутрішньої директорії системи, зокрема у директорії «Faces» файлів формату .jpg. Обрання пунктів меню та взаємодія з інтерфейсом користувача відбувається шляхом натискання на певні елементи керування інтерфейсу користувача.

Специфікація функціональних вимог представлена у вигляді діаграми прецедентів. На ній графічно показана сукупність прецедентів та суб'єктів, а також відношення між ними. Графічно діаграма прецедентів представлена на рисунку 3.1:

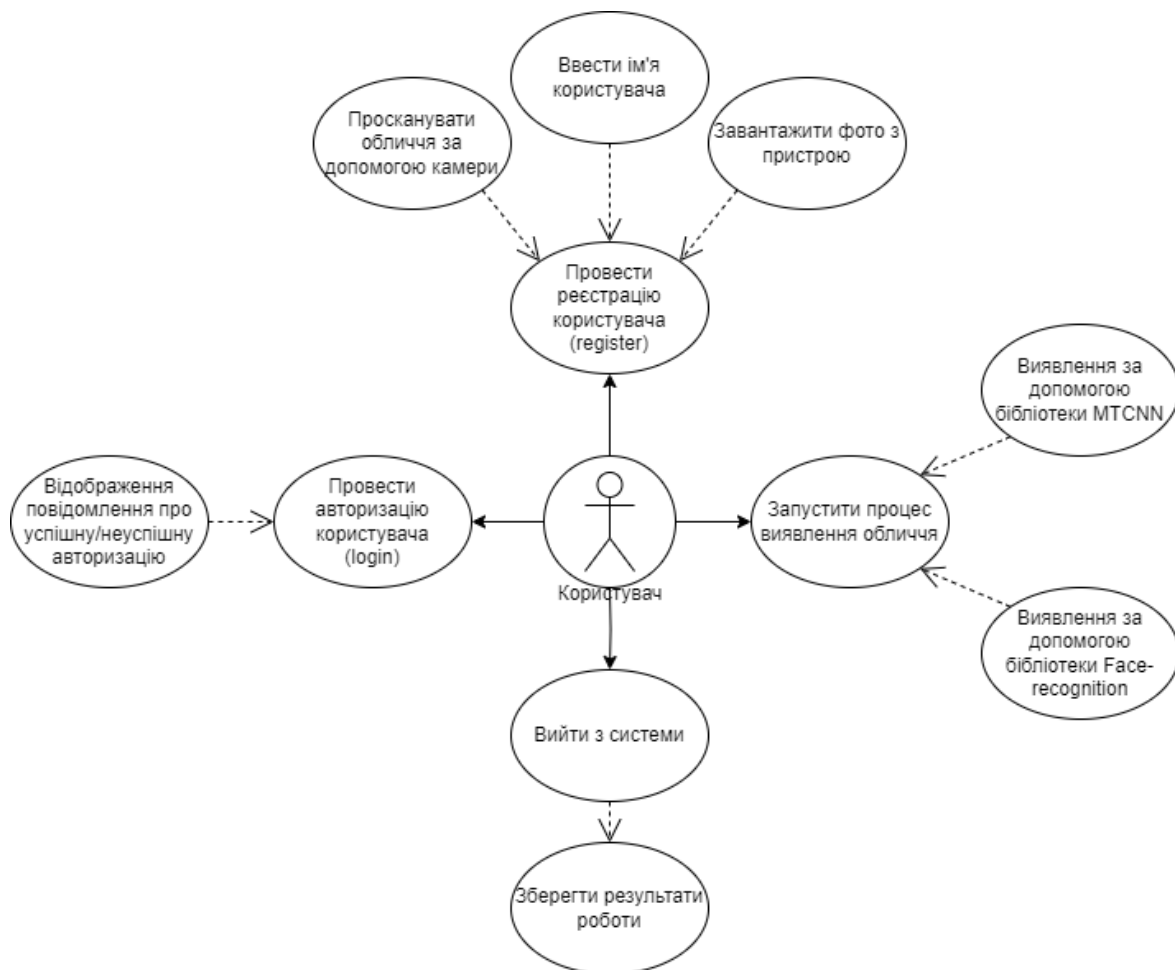


Рисунок 3.1 – Діаграма прецедентів

3.2 Внутрішнє проектування

3.2.1 Статична архітектура системи, моделювання залежностей

Статичну архітектуру системи можна логічно розділити на дві зони:

- нижня – зона користувацького меню на якій відображені усі основні пункти керування системою;
- верхня – зона відображення інформації про поточний стан системи та вивід необхідної інформації.

Схема взаємодії між цими двома зонами зображена на рисунку 3.2:

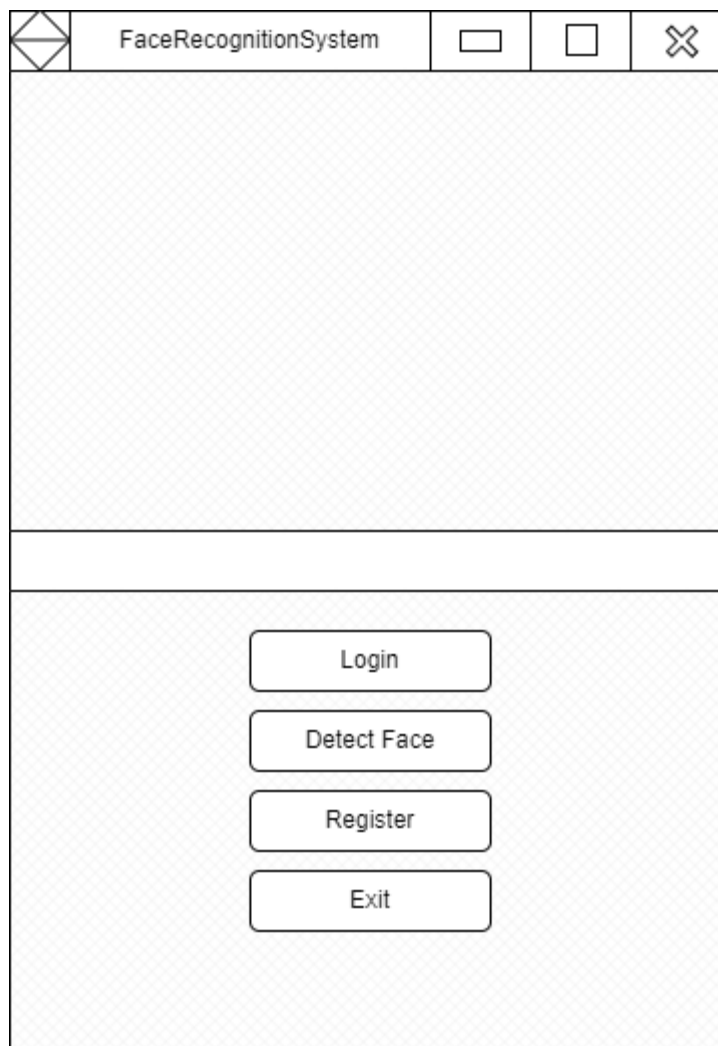


Рисунок 3.2 – Схема взаємодії зон керування системи

3.2.2 Структура внутрішнього сховища даних

Система вміщує структуру даних `videoCapture` типу `class`, що допомагає у керуванні відеопотоковим пристроєм.

Метод `update` дозволяє звертатися до відеокамери пристрою, зупиняючи або відтворюючи захват відеозображення.

Метод `start` дозволяє запускати відтворення відео в окремому потоці, що розвантажує основний процес.

Метод `read` дозволяє зчитувати кадр зображення з відеопотоку.

Метод `stop` зупиняє роботу з відеокамерою.

Метод `encode_faces` дозволяє отримати кодування усіх облич, що наявні у системі.

Метод `login`(обробник події натискання на кнопку) дозволяє виконати авторизацію користувача.

Метод `browse`(обробник події натискання на кнопку) дозволяє завантажити фотознімок з пристрою.

Метод `takeAShot`(обробник події натискання на кнопку) дозволяє зробити фотознімок за допомогою камери пристрою.

Метод `register`(обробник події натискання на кнопку) відкриває меню реєстрації нового користувача.

Метод `exit`(обробник події натискання на кнопку) дозволяє закрити систему.

Метод `detectMTCNN`(обробник події натискання на кнопку) дозволяє розпочати виявлення обличчя за допомогою алгоритмів бібліотеки MTCNN.

Метод `detectFR`(обробник події натискання на кнопку) дозволяє розпочати виявлення обличчя за допомогою алгоритмів бібліотеки Face-recognition.

Метод `detectFace`(обробник події натискання на кнопку) дозволяє порівняти обличчя, що вже наявні у системі з кандидатом на авторизацію.

У системі передбачена функція зберігання результату роботи у власній директорії у корінній папці “Faces”.

3.2.3 Особливості інтерфейсу користувача

Інтерфейс користувача – це засоби, які забезпечують зручність та ефективність взаємодії користувача з системою. З одного боку відбувається взаємодія користувача з інтерфейсом, а з іншого реакція системи на цю взаємодію. При розробці інтерфейсу користувача відсутній фіксований алгоритм від початку до кінця проектування.

За час проектування інтерфейсу користувача враховувались декілька головних принципів, які прослідковуються упродовж розробки усієї програми, зокрема привабливий та зрозумілий дизайн інтерфейсу, що використовує естетично приємні кольори та інтегрується із загальним виглядом системи. Використовуються корисні

повідомлення, які допомагатимуть у роботі з системою. Використовуються зрозумілі терміни для повідомлень. За необхідності виводиться окреме вікно повідомлення з вказаним типом помилки. Забезпечення користувачу можливості вільно орієнтуватися у системі, при цьому уникаючи ситуацій при яких користувач може зіткнутися з помилками. Створення легкого інтуїтивного інтерфейсу до якого користувач може швидко звикнути та використовувати усі наявні можливості системи. Узгодженість системи відображається у тому, що користувач може використовувати прийоми роботи набуті у роботі з іншими системами. Покращена організація інтерфейсу для більш якісної візуалізації шляхом використання груп об'єктів.

Одним з найважливіших моментів при розробці інтерфейсу користувача є колір. Вибір кольору може впливати на сприйняття та зручність використання системи. Психологічні реакції людини на колір можуть викликати як негативне, так і позитивне відношення до системи. Саме тому головним принципом вибору кольору є його дружність та привабливість для більшості людей[15].

За основу під час проектування інтерфейсу було взято бібліотеку для створення сучасних користувацьких інтерфейсів CustomTkinter. Ця бібліотека є розширенням стандартної бібліотеки графічного інтерфейсу користувача для мови програмування Python. За допомогою CustomTkinter можна налаштувати, наприклад, рамки елементів керування, або ж заокруглені кнопки. До того ж, він підтримує світлу та темну тему, яку можна встановити вручну або керувати режимом зовнішнього вигляду системи.

Налаштування графічних елементів також є досить важливим елементом інтерфейсу користувача. Вирівнювання полів, їх розташування повинне бути згруповане та відповідати певному алгоритму розміщення. Вирівнювання елементів керування має бути однакове по всій системі.

На основі сказаного вище було розроблено ескізи головного екрану системи.
Зображення головного екрану продемонстроване на рисунку 3.3:

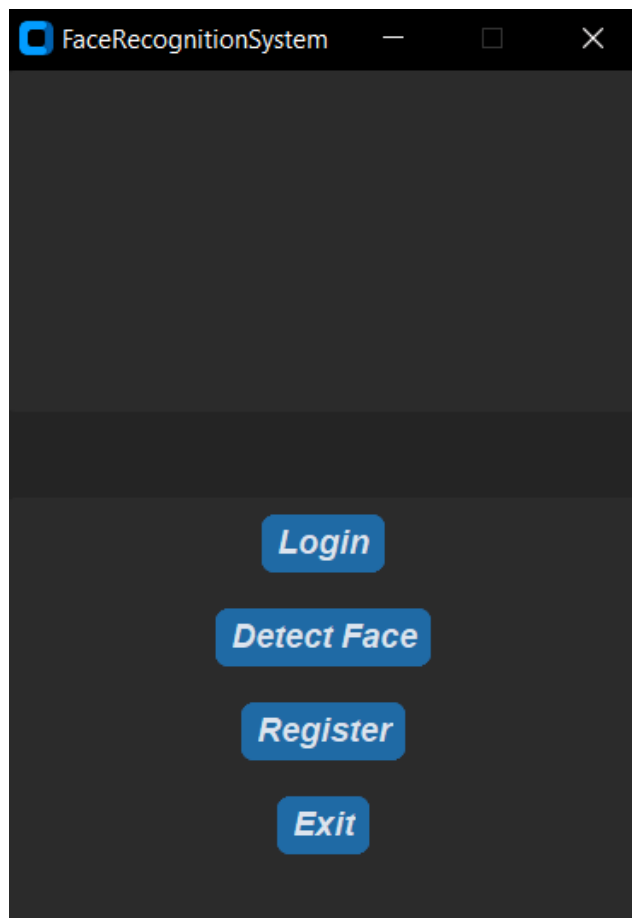


Рисунок 3.3 – Зображення головного екрану

Зображення головного екрану при натисканні кнопки «Detect Face» продемонстроване на рисунку 3.4:

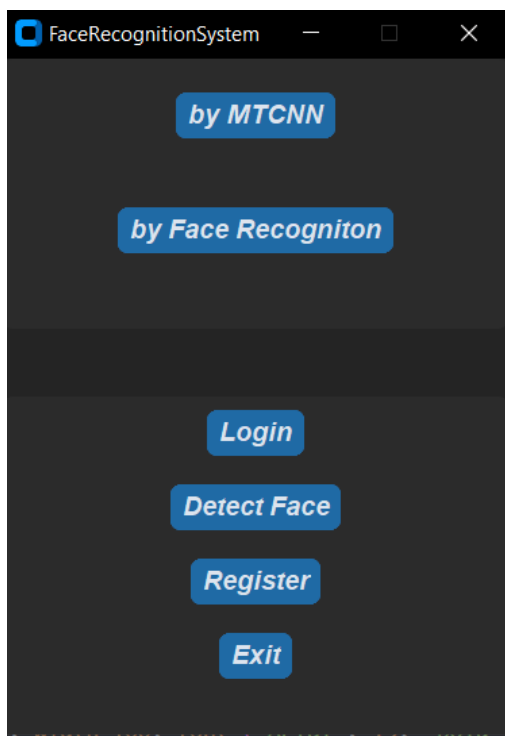


Рисунок 3.4 – Зображення екрану при натисканні кнопки «Detect Face»

Зображення головного екрану при натисканні кнопки «Register» продемонстроване на рисунку 3.5:

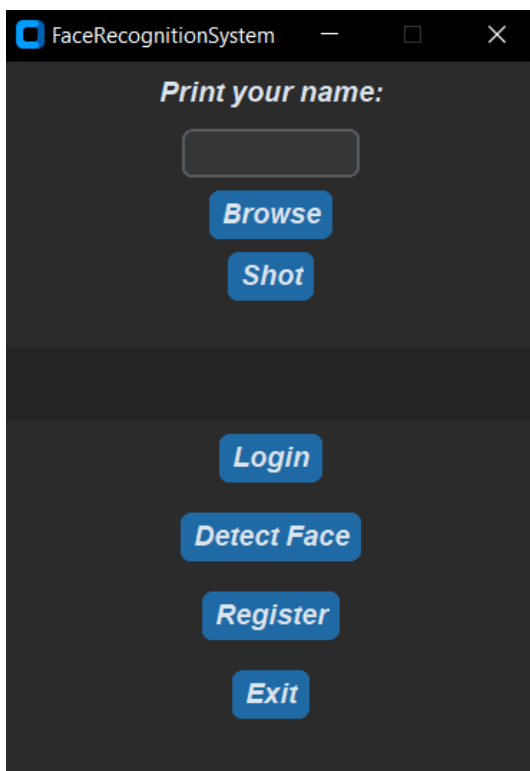


Рисунок 3.5 – Зображення екрану при натисканні кнопки «Register»

3.2.4 Моделювання процесу виконання операцій

Діаграма діяльності системи при авторизації користувача зображена на рисунку

3.6:

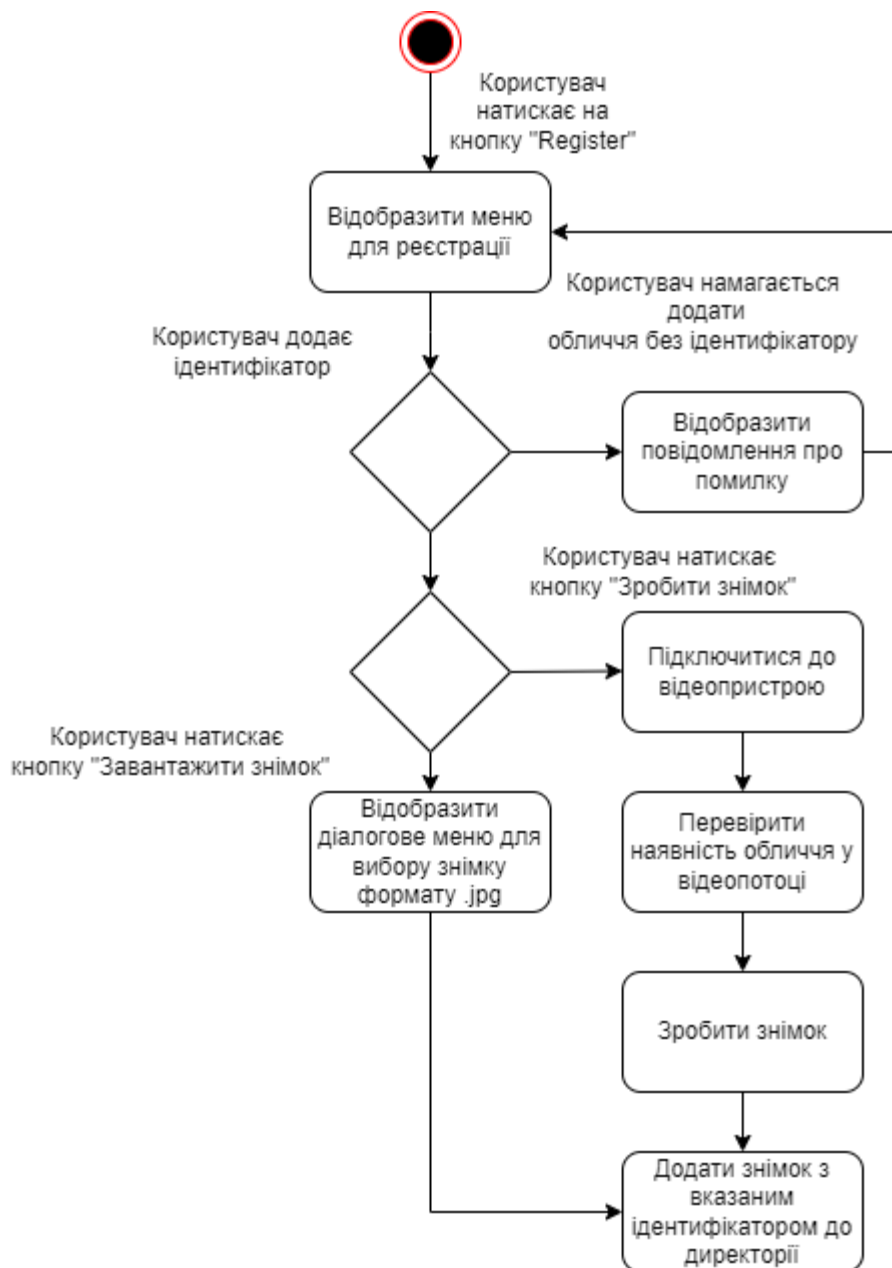


Рисунок 3.6 – Діаграма діяльності при реєстрації нового користувача

Початковим станом системи авторизації шляхом розпізнавання обличчя є головний екран додатку. Після натискання користувачем елементу керування, який відповідає за реєстрацію нового користувача, йому пропонується обрати один з двох варіантів завантаження фотознімку. Перший варіант – це зробити знімок за допомогою

камери пристрою, вказавши ідентифікатор за яким буде збереженоо файл. Другий варіант – це завантажити фотознімок формату .jpg з пристрою на якому працює система. В цьому випадку ідентифікатор також необхідний для збереження файлу.

3.3 Обґрунтування вибору мови програмування Python

Серед поширених мов програмування, які можуть використовувати подібні задачі досить ефективно є такі як: JavaScript, C++, Python.

Для реалізації поставленої задачі була обрана мова Python, яка має численні переваги для реалізації подібних задач. Серед них:

Зручність та Простота. Python відомий своєю простотою та легкістю в освоєнні. Це робить його досить доступним для широкого кола розробників, навіть тих, хто не має глибоких знань в області програмування.

Широкий Вибір Бібліотек. Python має багато бібліотек та фреймворків для машинного навчання та обробки зображень, що значно полегшує розробку алгоритмів розпізнавання обличчя. Наприклад, OpenCV, Dlib, face_recognition, MTCNN.

Масштабованість та Спільнота. Python є мовою, яка широко використовується у сфері наукових досліджень, машинного навчання та штучного інтелекту. Це означає наявність великої та активної спільноти, що сприяє обміну знаннями та розвитку інструментів для розпізнавання обличчя.

Інтеграція з Іншими Мовами та Технологіями. Python добре взаємодіє з іншими мовами програмування, що дозволяє інтегрувати різноманітні бібліотеки та технології для покращення роботи системи розпізнавання обличчя.

Широкий Вибір Інструментів та Ресурсів. Python надає доступ до різноманітних інструментів та ресурсів, що полегшує роботу з даними, обробкою зображень, розгортанням систем та іншими аспектами розробки.

Python має низький поріг входу та досить простий у розумінні, що дозволяє зосередитись саме на дослідницькій частині та розробці системи розпізнавання обличчя у реальному часі.

3.4 Тестування

Тестування – процес визначення або перевірки функціональності системи на відповідність певним вимогам з метою виявлення помилок при певних вхідних даних.

3.4.1 Тестування білою скринькою

Проведемо тестування функції login(), яка відповідає за надання або заборону доступу до системи для користувача.

Вхідні дані:

- список наявних зображень формату .jpg зареєстрованих користувачів системи корінного каталогу /faces;
- зображення з відеокамери для ідентифікації та авторизації кандидата на вхід до системи.

Вихідні дані :

- надання або заборона доступу до системи для кандидата авторизації.

Нижче наведено текст функції login():

```
def login():
    faces = encode_faces()
    encoded_faces = list(faces.values())
    faces_name = list(faces.keys())
    videostream = videoCapture(0)
    videostream.start()
    face_locations = []
    while face_locations == []:
        frame = videostream.read()
        face_locations = face_recognition.face_locations(frame)
        print(face_locations)
    unknown_face_encodings = face_recognition.face_encodings(frame, face_locations)
    videostream.stop()
    cv2.destroyAllWindows()
    index = 0
    for face_encodings in encoded_faces:
        result = face_recognition.compare_faces(face_encodings, unknown_face_encodings)
        if result[0] == True:
            print(faces_name[index])
            inputname.configure(text= 'Hello ' + faces_name[index] + 'accessallowed!')
            inputname.pack()
            break
    else:
```

```

inputname.configure(text23= 'Access denied!')
inputname.pack()
index24+=1

```

Зображення блок-схеми функції login() наведено на рисунку 3.7:

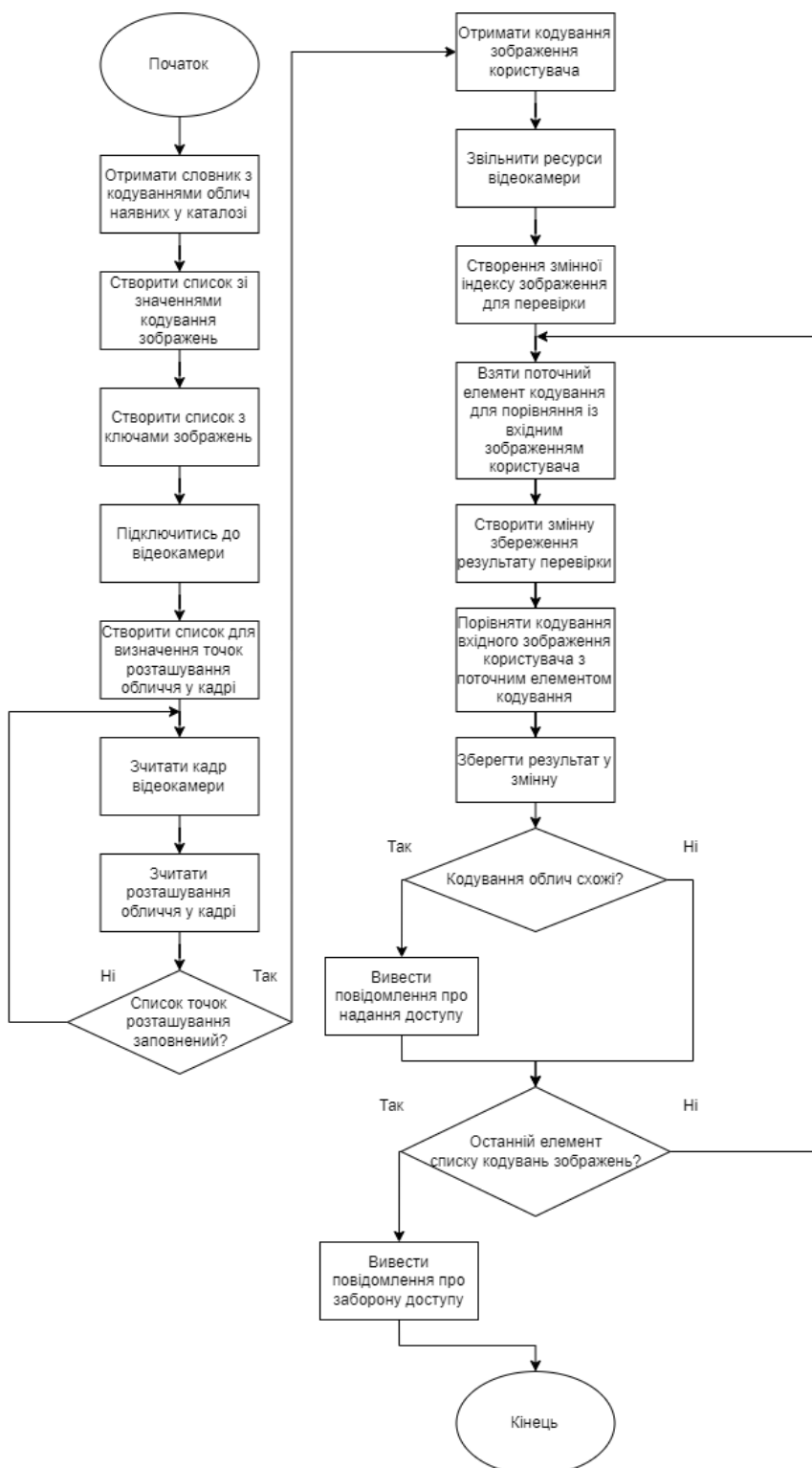


Рисунок 3.7 – Блок-схема функції login()

Тести до функції login() наведено у таблиці 3.1:

Таблиця 3.1 Тести до функції login()

№ тесту	Вхідні значення		Вихідні значення
	Список наявних зображень	Зображення з відеокамери	
1	2	3	4
1.	Список зображень, серед яких наявне обличчя кандидату для авторизації	Зображення користувача, який вже зареєстрований у системі	Надання доступу до системи
2.	Список зображень, серед яких немає обличчя кандидату для авторизації	Зображення користувача, який ще не зареєстрований у системі	Заборона доступу до системи
3.	Список зображень, серед яких наявне обличчя кандидату для авторизації	Зображення на якому не має обличчя	Заборона доступу до системи

Тестування методом покриття операторів описано у табл. 3.2:

Таблиця 3.2 Тестування методом покриття операторів

№ тесту	Номер оператора																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	+	+	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	+	+	+	+	-	-	+
2	+	+	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	-	-	-	-	+	+	+
3	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-

При виконанні тестів, кожен оператор виконався хоча б один раз.

Тестування методом покриття рішень описано у табл. 3.3:

Таблиця 3.3. Тестування методом покриття рішень

№ тесту	Номер рішення					
	6-	6+	13+	13-	16+	16-
1	-	+	+	-	-	-
2	-	+	-	+	+	+
3	+	-	-	-	-	-

При виконанні тестів, кожен напрямок переходу був реалізований хоча б раз.

3.4.2 Тестування чорною скринькою

Тестування чорною скринькою проведемо на основі опису роботи функцій програми. Виконаємо декілька наступних пунктів.

Двічі натиснемо на іконку .exe файлу на пристрої, тим самим завантаживши систему. Зображення головного екрану системи наведено на рисунку 3.8:

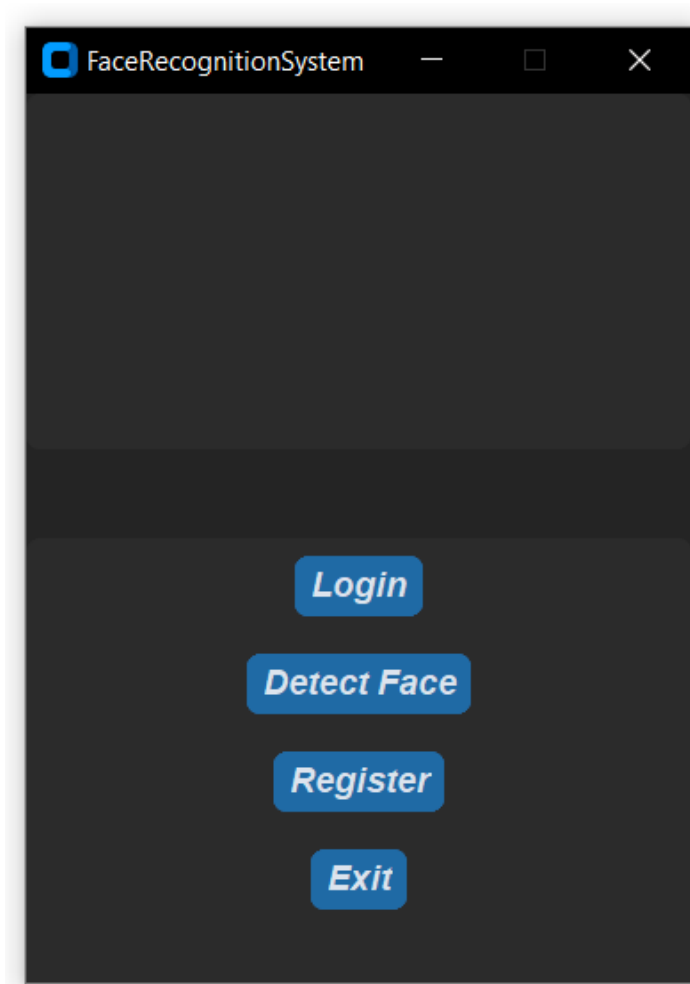


Рисунок 3.8 – Зображення головного екрану системи

Спробуємо виконати реєстрацію нового користувача системи натиснувши на кнопку «Register», в результаті чого відкриється меню, що наведено на рисунку 3.9:

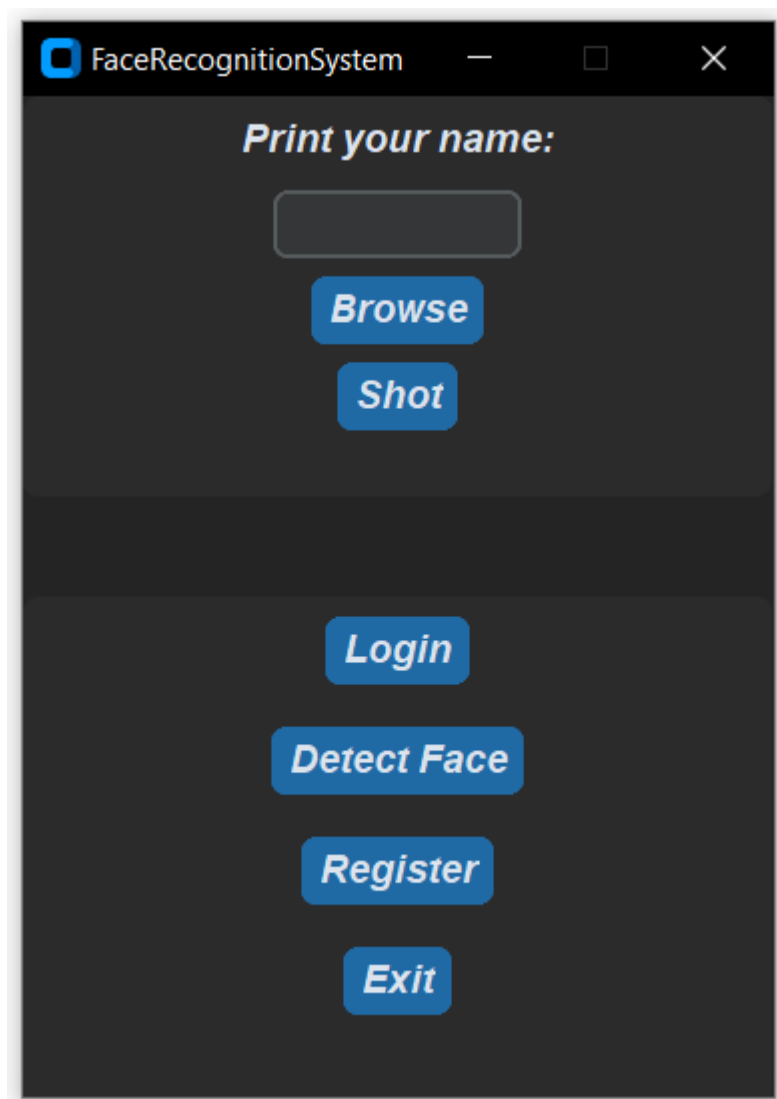


Рисунок 3.10 – Зображення меню реєстрації нового користувача системи

Введемо ідентифікатор нового користувача та натиснемо пункт меню «Shot», в результаті чого за допомогою камери виконається фото та збережеться у корінній папці системи. Результати роботи наведені на рисунку 3.11:

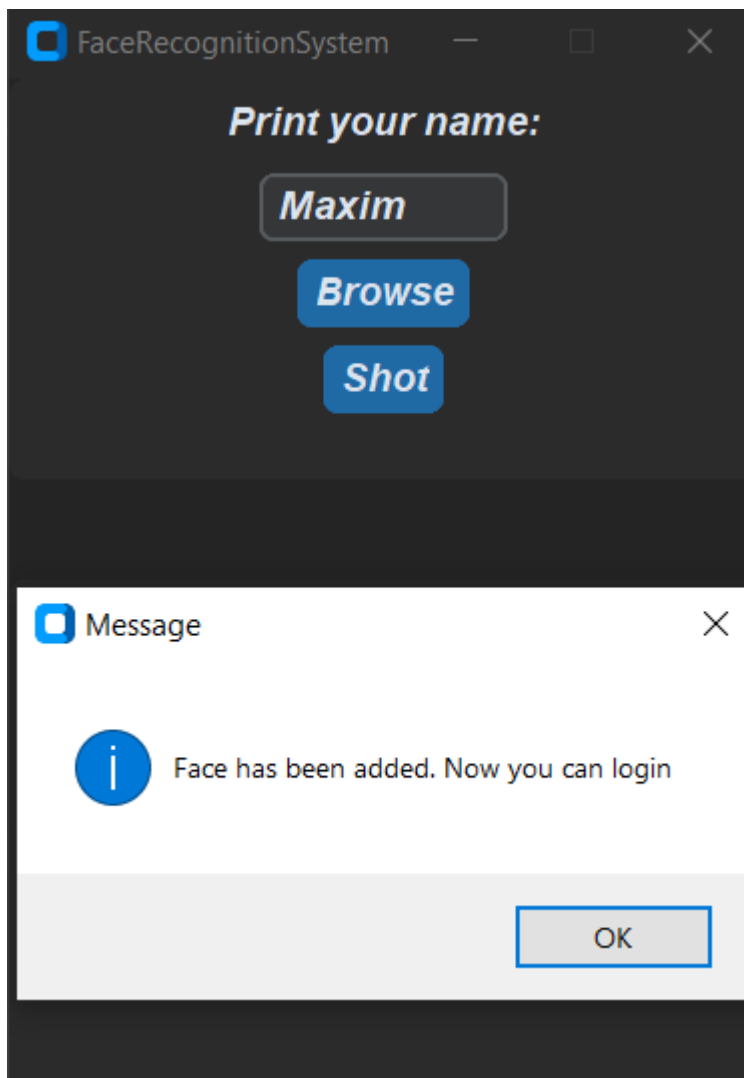


Рисунок 3.12 – Виведення повідомлення про реєстрацію нового користувача системи

В корінній папці відображається новий користувач системи з ідентифікатором, який було вказано під час реєстрації. Результати роботи наведені на рисунку 3.13:

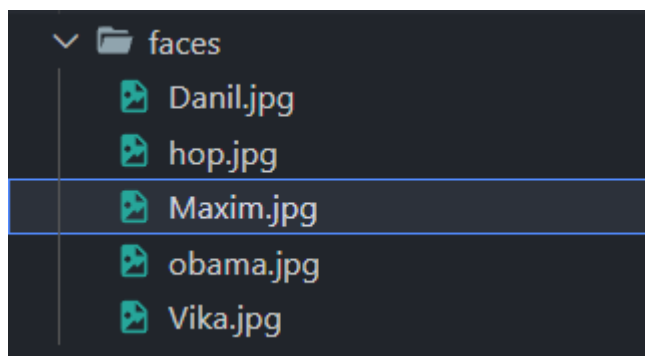


Рисунок 3.13 – Відображення нового користувача системи

Спробуємо завантажити фото з пристрою для реєстрації нового користувача. Для цього натиснемо кнопку «Browse» та оберемо файл, який не відповідає формату. Результати роботи наведені на рисунку 3.14:

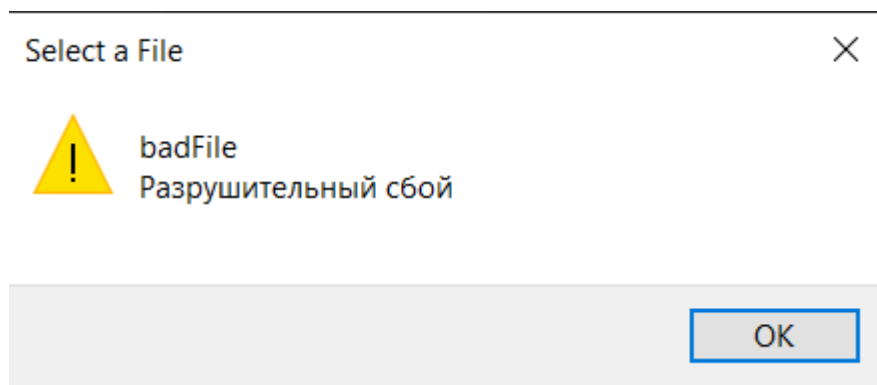


Рисунок 3.14 – Виведення повідомлення про обрання файлу не відповідного формату

Оберемо зображення формату .jpg та задамо йому ідентифікатор. Результати роботи наведені на рисунку 3.15:

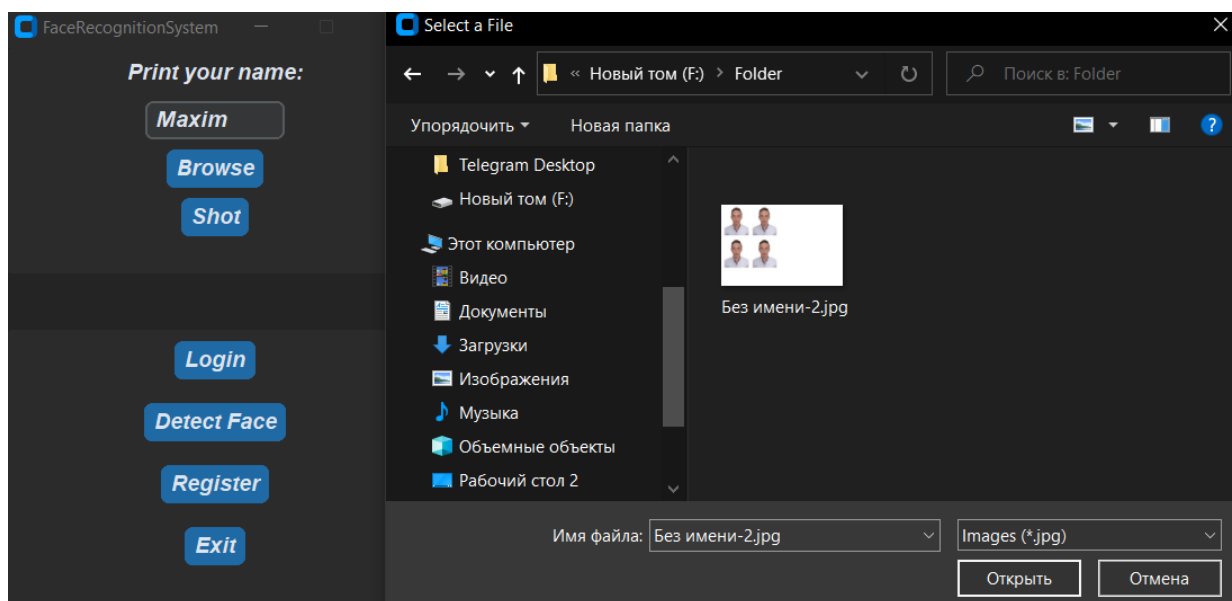


Рисунок 3.15 – Вікно завантаження зображення .jpg з пристрою

Нове обличчя зареєстровано, тож виконаємо вхід до системи натиснувши на кнопку «Login». Результати роботи наведені на рисунку 3.16:

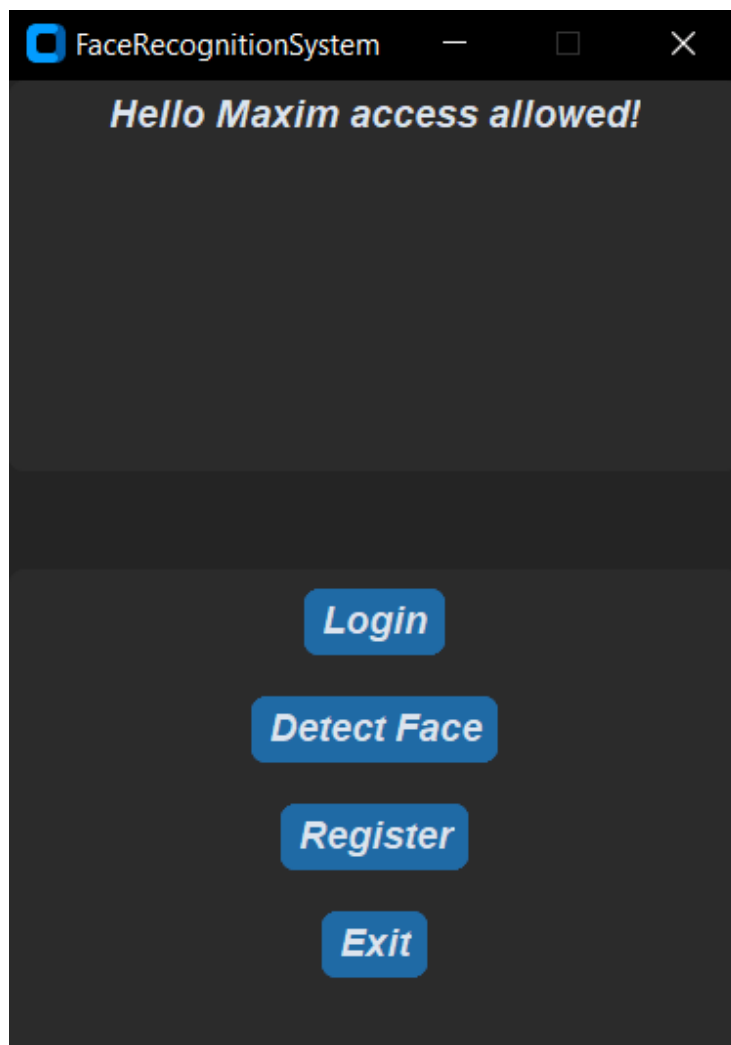


Рисунок 3.16 – Відображення повідомлення про успішний вхід до системи

Спробуємо піднести до камери обличчя, якого немає в системі та виконати вхід тим самим перевіривши реакцію системи. Результати роботи наведені на рисунку 3.17:

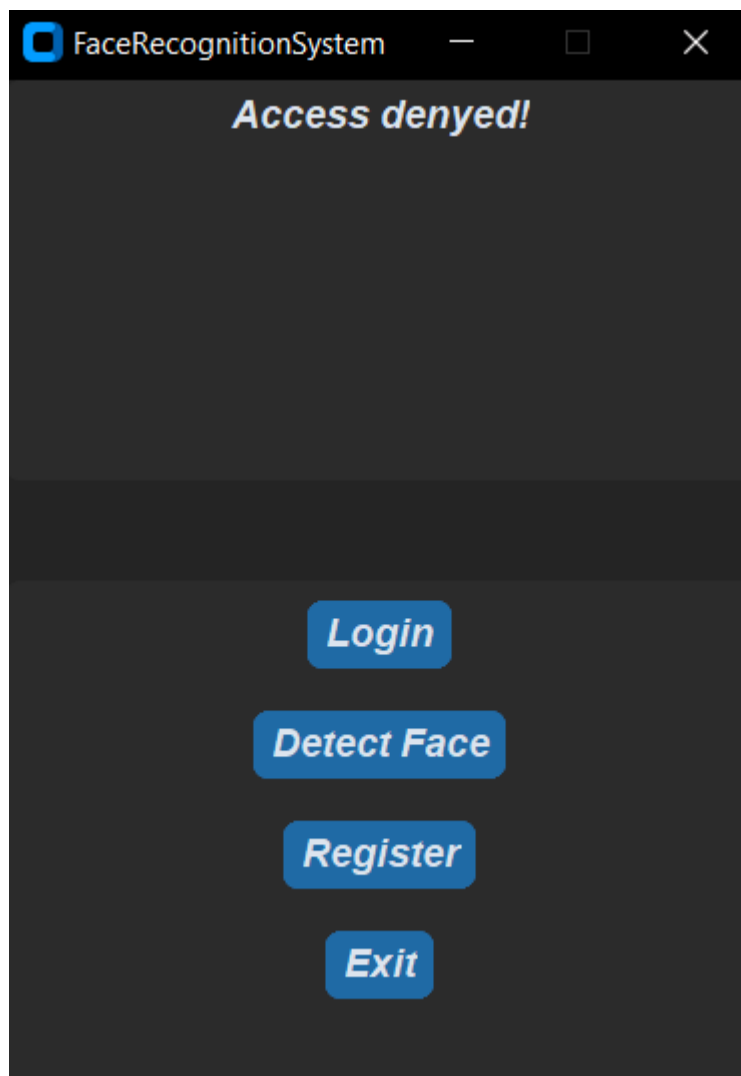


Рисунок 3.17 – Відображення повідомлення про заборону доступу до системи

Спробуємо перейти до меню детекції обличчя натиснувши на кнопку «Detect Face». Результати роботи наведені на рисунку 3.18:

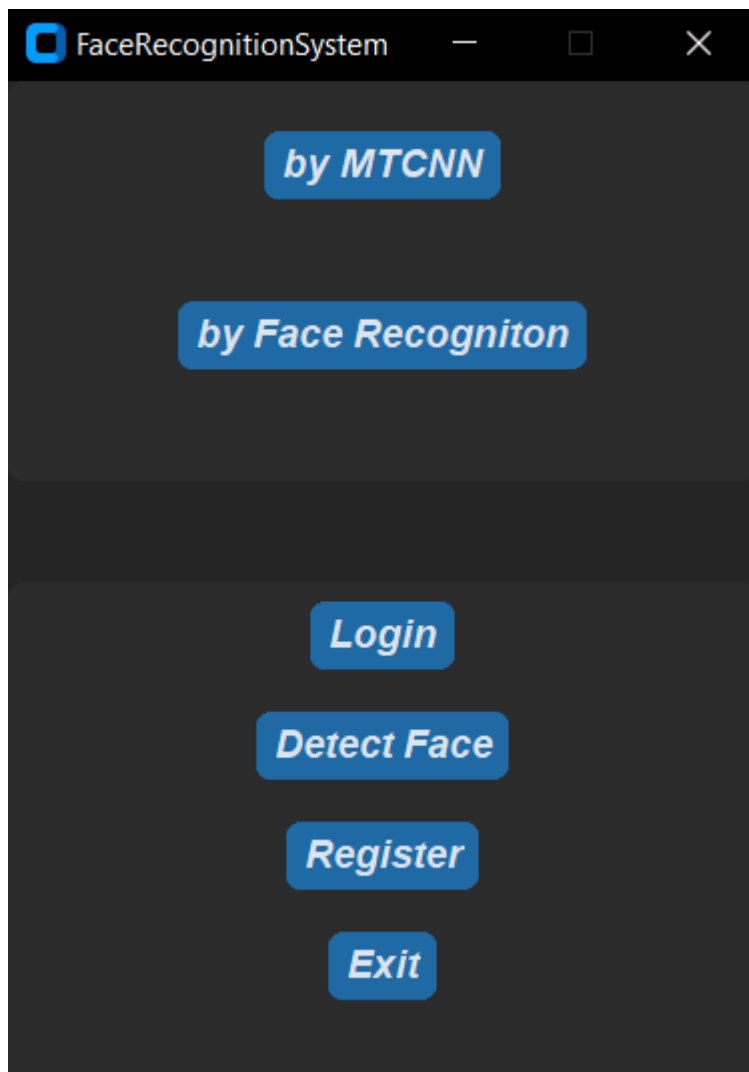


Рисунок 3.18 – Відображення пункту меню детекції обличчя

Натиснемо пункт меню «by MTCNN» для детекції обличчя за допомогою бібліотеки каскадних нейронних мереж. Результати роботи наведені на рисунку 3.19:

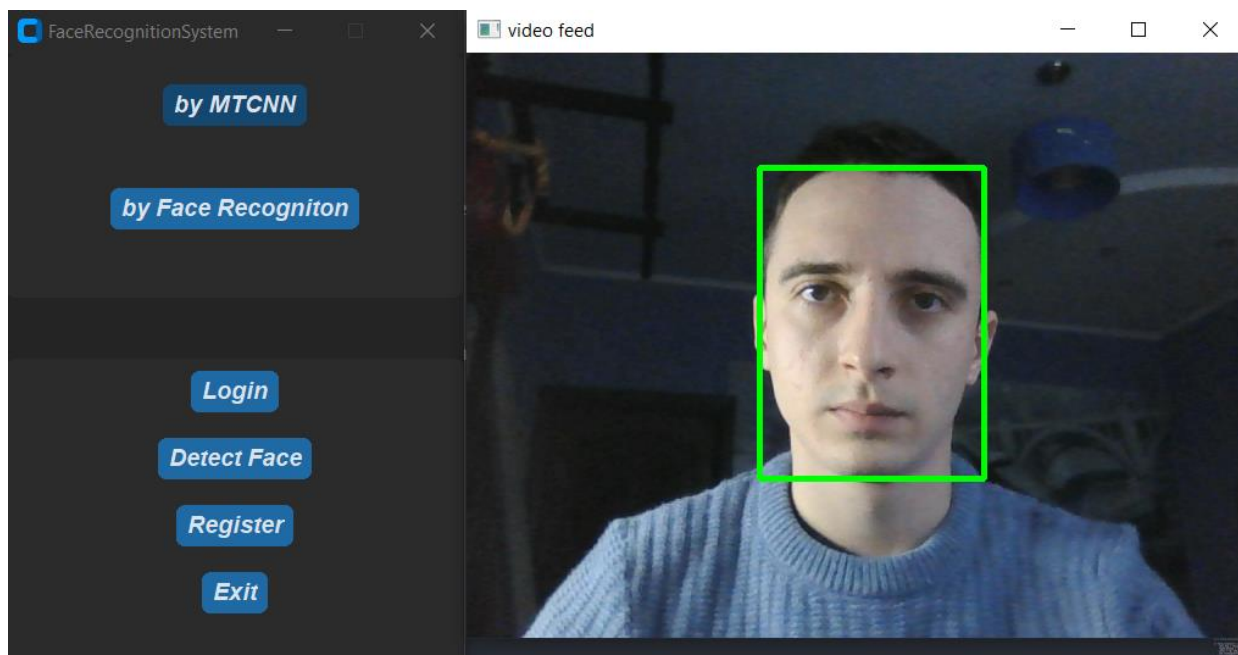


Рисунок 3.19 – Детекція обличчя бібліотекою MTCNN

Якщо виконати авторизацію і при цьому система через камеру не буде бачити обличчя, то розпізнавання почнеться тільки, після того як обличчя з'явиться в полі зору камери. При роботі з декількома обличчями система розпізнає перше зчитане та додасть його до каталогу. Якщо намагатися додати файл іншого формату відмінного від .jpg, виведеться повідомлення про помилку. При цьому додавати файл без вказаного ідентифікатора у полі «name» не можливо. Система не дасть цього зробити і виведе повідомлення про помилку.

Як бачимо основні функції працюють без помилок, перейдемо до безпосереднього налагодження програми.

3.4.3 Налагодження програми

Під час налагодження програми було виявлено ряд синтаксичних, семантичних та логічних помилок. Переважно зустрічалися помилки звернення до пустого списку, відсутність перевірок успішного запуску камери. Помилки було виправлено додаванням умов перевірки стану системи, обробкою виняткових ситуацій.

Переважну більшість помилок було виправлено за допомогою внутрішніх інструментів, що наявні в середовищі розробки Visual Studio Code та додаткових

розширень для рефакторингу коду. Точки переривання допомагали визначати значення змінних в конкретних умовах процесу виконання коду системи. Протокол налагодження програми наведений у таблиці 3.4:

Таблиця 3.4 Протокол налагодження програми

Опис помилки	Опис ситуації	Способи усунення	Дії, що були застосовані для усунення
1	2	3	4
Звернення до пустого списку	Якщо під час роботи системи не було виявлено обличчя у камері, то подальша робота системи велась з пустими списками ембендингів	Додати перевірку на наповненість списку	Додати перевірку на наповненість списку <pre>while face_locations == []: frame = videostream.read() face_locations = face_recognition.face_locations(frame)</pre>
Помилка збереження файлу без імені	Якщо користувач обрав зображення та не ввів	Створення повідомлення про обов'язковість заповнення поля	Створення повідомлення про обов'язковість заповнення поля ідентифікатора <pre>if len(name.get()) == 0: messagebox.showinfo('Error', 'There are is no name in text field')</pre>

1	2	3	4
	ідентифікатор виникала помилка при збереженні файлу без імені	ідентифікатора	
Помилка використання ресурсів	Після відпрацювання камери ресурси не звільнялися, що призводило до збільшення їх використання	Звільнення ресурсів відеокамери	Звільнення ресурсів відеокамери <pre>cap.release() cv2.destroyAllWindows()</pre>

Висновки до третього розділу

Реалізована структура проекту, що має свої чіткі функції та області за які вони відповідають, описано процес зовнішнього та внутрішнього проектування, проведено тестування та налагодження програми. Система повністю підходить для подальшого дослідження ефективності алгоритмів бібліотек розпізнавання обличчя у реальному часі. Вдалося досягти відповідності початковим вимогам до системи, що спрощує виконувати експерименти. За потреби система може бути масштабована для подальшого її використання за межами наукових досліджень шляхом доповнення її функціями безпосереднього надання доступу після авторизації користувачем, що допоможе вирішувати реальні більш складні завдання.

РОЗДІЛ 4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ БІБЛІОТЕК ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

4.1 Результати експериментів

Метою проведення експериментів є визначення ефективності виявлення обличчя за різних умов бібліотек розпізнавання обличчя MTCNN та Face-recognition. Для вирішення цього завдання проведемо п'ять експериментів за різних умов навколишнього середовища:

- експеримент №1 – робота алгоритмів за ідеальних умов;
- експеримент №2 – робота алгоритмів при низькому рівні освітлення;
- експеримент №3 – робота алгоритмів, коли обличчя знаходиться під кутом до камери;
- експеримент №4 – робота алгоритмів при наявності перешкод на обличчі;
- експеримент №5 – робота алгоритмів при зміні дистанції до камери.

Як об'єкт для проведення експерименту щодо алгоритму виявлення обличчя в режимі реального часу на кадрі вибрано зображення з пристрою відеокамери, яке має наступні характеристики:

- роздільна здатність: 640 x 480;
- ширина: 640 пікселів;
- висота: 480 пікселів;
- горизонтальна роздільна здатність: 96 точок на дюйм;
- роздільна здатність по вертикалі: 96 точок на дюйм;
- глибина кольору: 24.

Експерименти будуть проводитись за допомогою розробленої системи авторизації користувача шляхом виявлення та розпізнавання обличчя у режимі реального часу. Оцінка ефективності буде визначатись на основі отриманої статистики використання ресурсів від системи та запропонованих метрик у розділі 2.

Умови проведення експерименту №1 будуть наступні:

- рівень освітлення: достатній, наявне сонячне освітлення та додаткове освітлення ламп в кімнаті;
- час доби: 14.00;
- кут обличчя до камери: фронтальне зображення;
- перешкоди між камерою та обличчям: відсутні;
- дистанція до камери: 60 см.

Зображення з відеокамери продемонстроване на рисунках 4.1, 4.2:

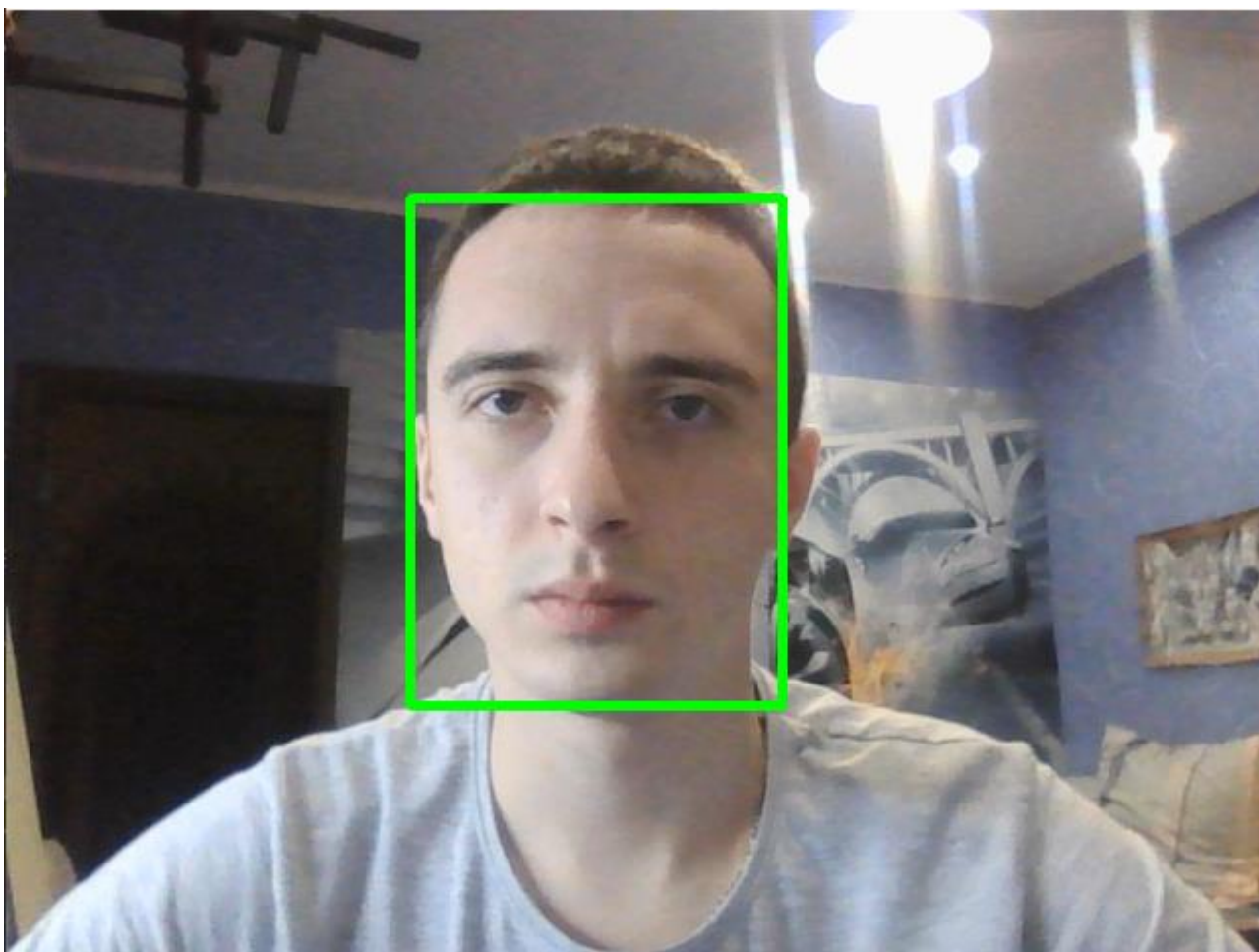


Рисунок 4.1 – Зображення з відеокамери експерименту №1 для алгоритмів бібліотеки
MTCNN

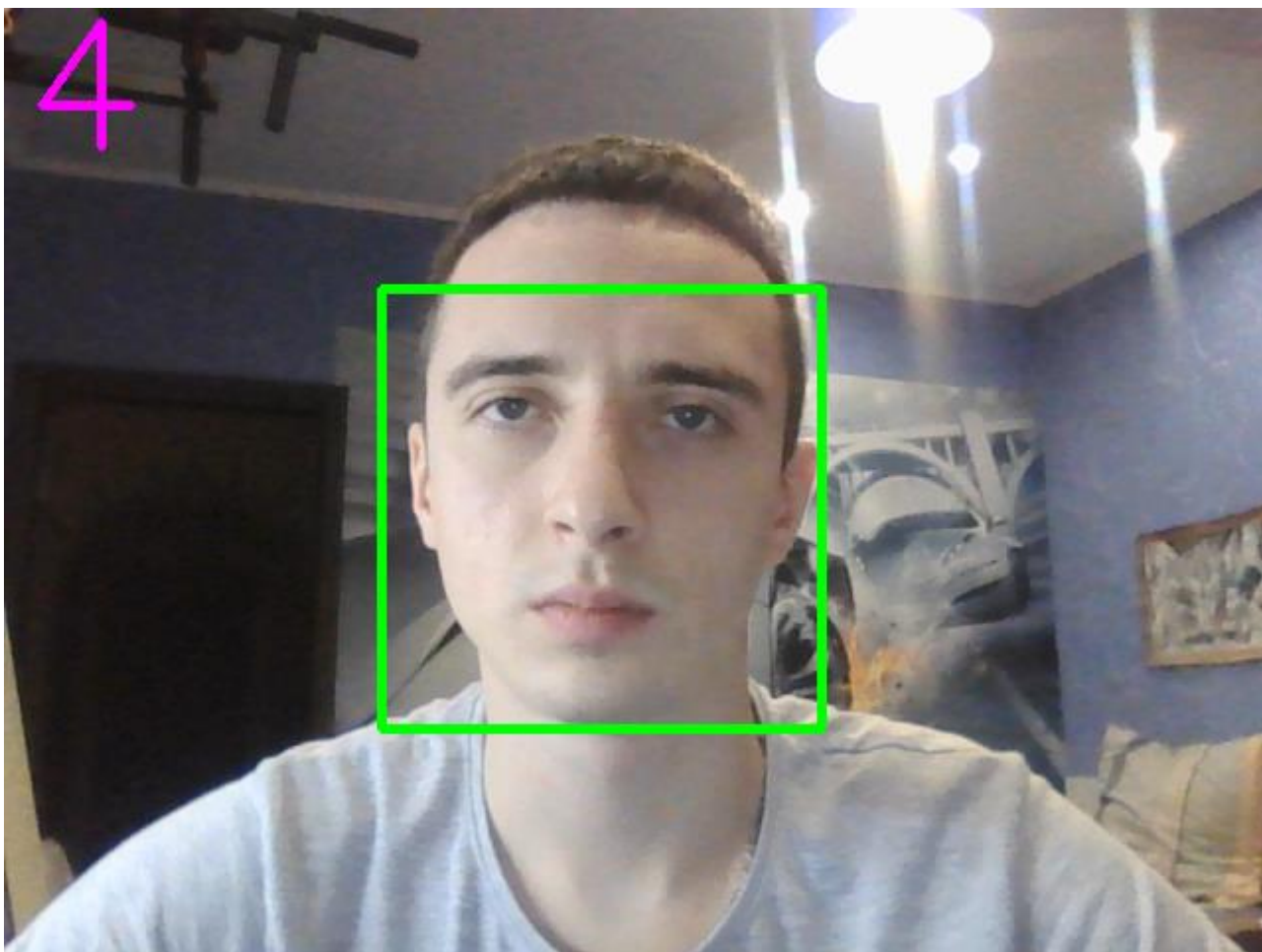


Рисунок 4.2 – Зображення з відеокамери експерименту №1 для алгоритмів бібліотеки Face-recognition

Для рисунку 4.1 та 4.2 було отримано дані, що зведено у таблиці 4.1:

Таблиця 4.1 Використання системою ресурсів під час експерименту №1

	Алгоритми бібліотеки MTCNN	Алгоритми бібліотеки Face- recognition	Різниця
Час виявлення обличчя, с	0.8	0.18	0.62
Використання RAM, мб	504.2	453.12	51,08
Використання ресурсів процесора, %	16.4	12.0	4,4

Умови проведення експерименту №2 будуть наступні:

- рівень освітлення: низький, відсутнє сонячне та додаткове освітлення;
- час доби: 20.00;
- кут обличчя до камери: фронтальне зображення;
- перешкоди між камерою та обличчям: відсутні;
- дистанція до камери: 60 см.

Зображення з відеокамери продемонстроване на рисунку 4.3, 4.4:

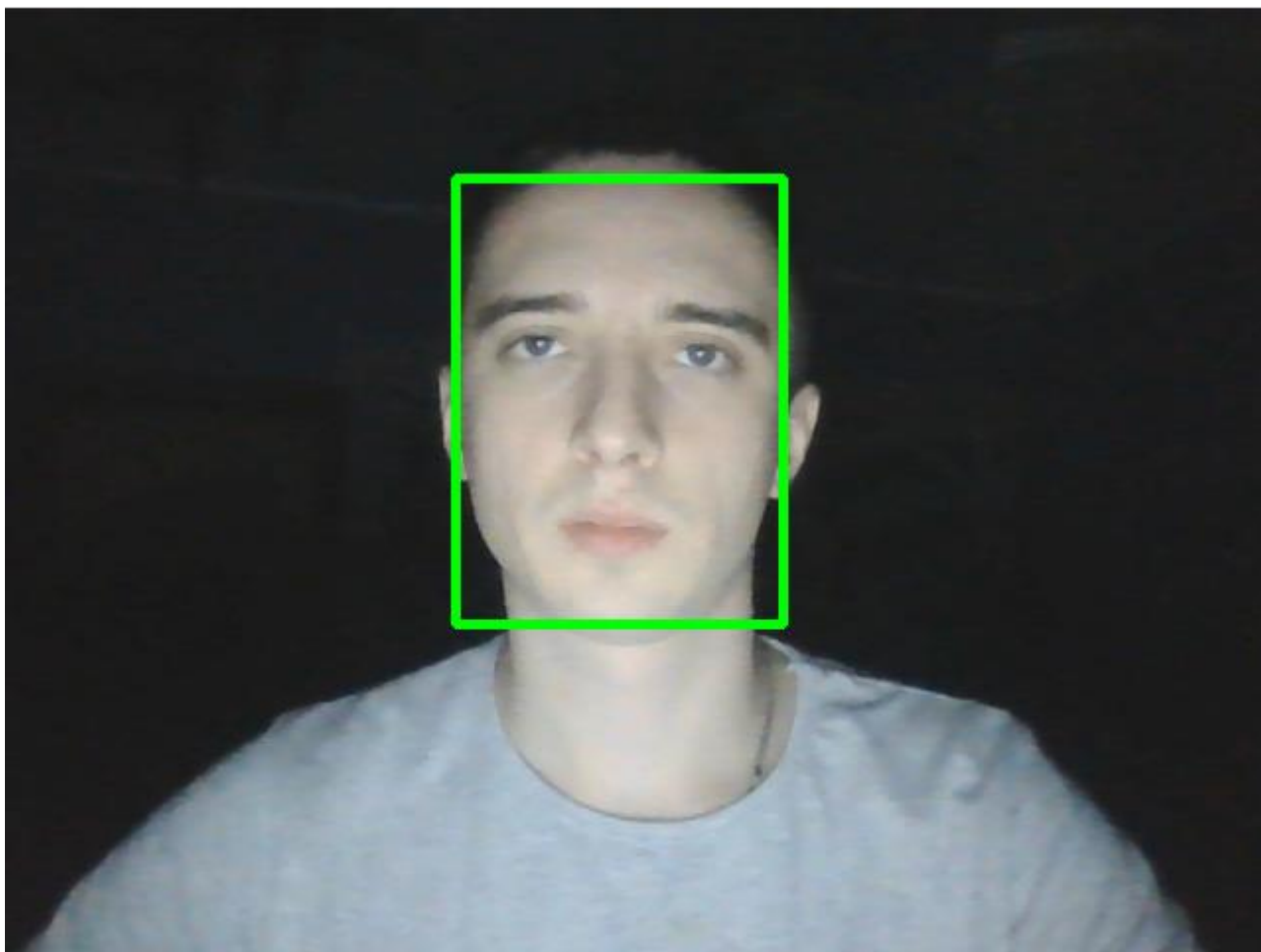


Рисунок 4.3 – Зображення з відеокамери експерименту №2 для алгоритмів бібліотеки
MTCNN

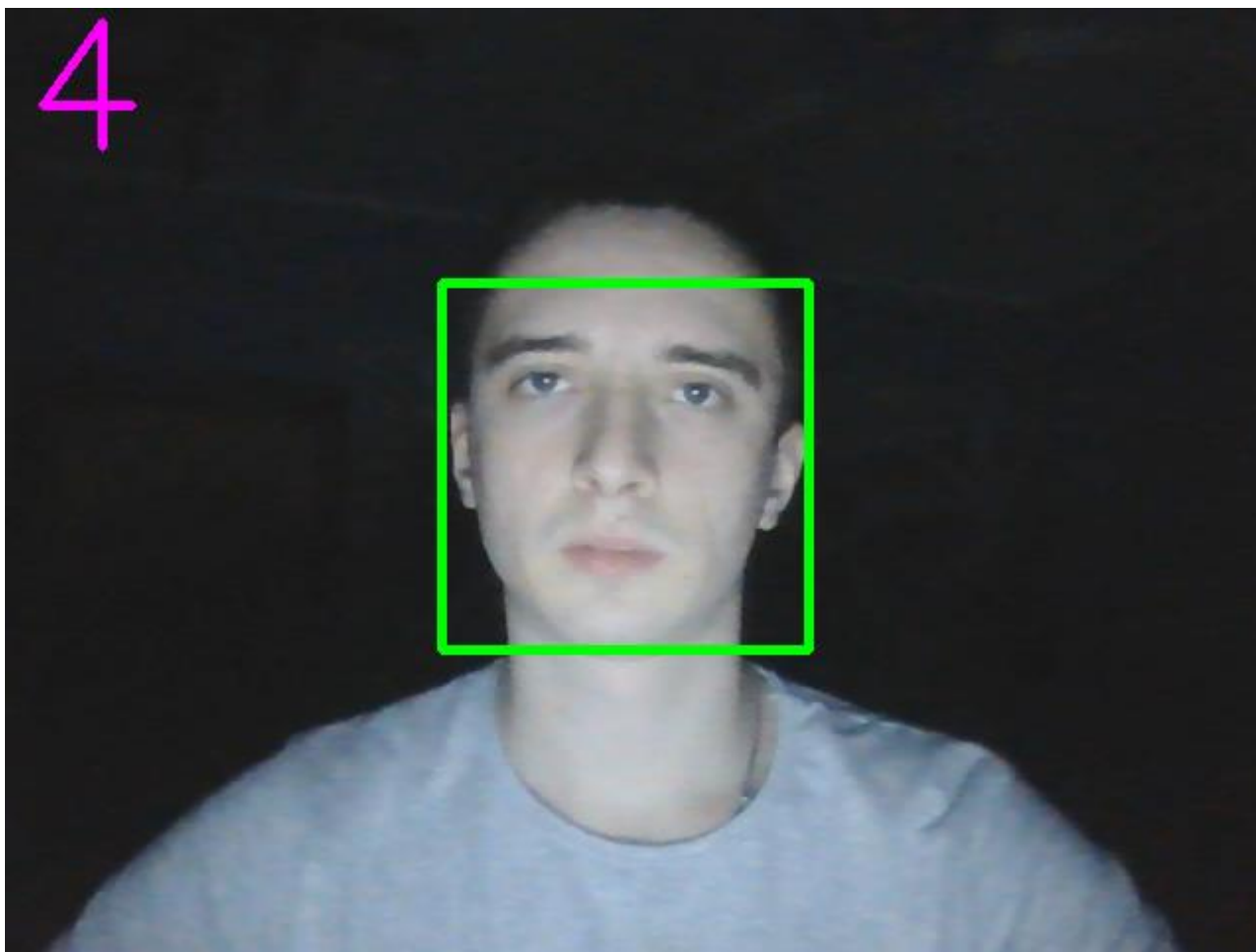


Рисунок 4.4 – Зображення з відеокамери експерименту №2 для алгоритмів бібліотеки Face-recognition

Для рисунку 4.3 та 4.4 було отримано дані, що зведено у таблиці 4.2:

Таблиця 4.2 Використання системою ресурсів під час експерименту №2

	Алгоритми бібліотеки MTCNN	Алгоритми бібліотеки Face- recognition	Різниця
Час виявлення обличчя, с	0.898	0.21	0,688
Використання RAM, мб	537.5	464.98	72,52
Використання ресурсів процесора, %	17.3	12.6	4.7

Умови проведення експеременту №3 будуть наступні:

- рівень освітлення: достатній, наявне сонячне освітлення та додаткове освітлення ламп в кімнаті;
- час доби: 14.00;
- кут обличчя до камери: 90 градусів;
- перешкоди між камерою та обличчям: відсутні;
- дистанція до камери: 60 см.

Зображення з відеокамери продемонстроване на рисунку 4.5, 4.6:

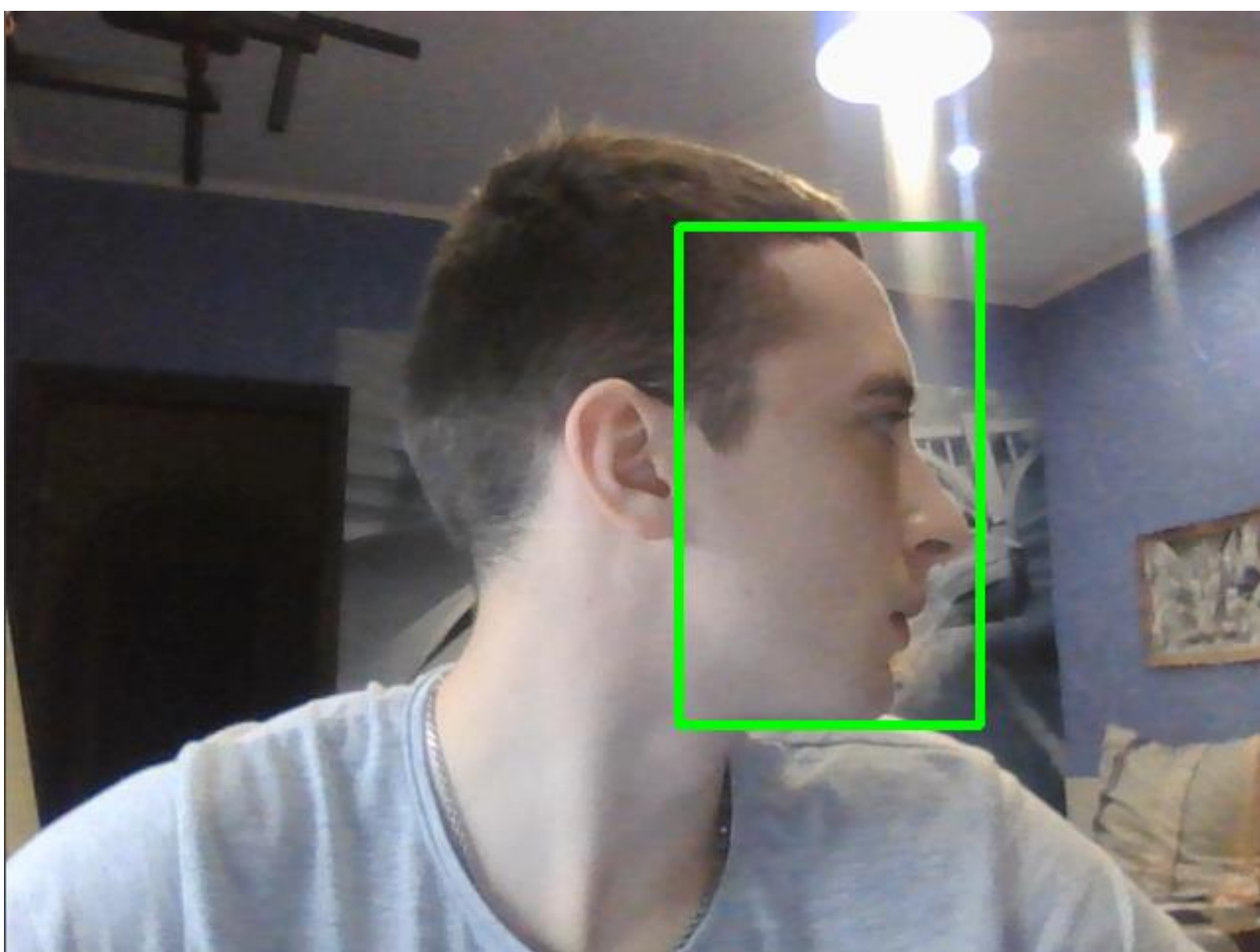


Рисунок 4.5 – Зображення з відеокамери експеременту №3 для алгоритмів бібліотеки
MTCNN

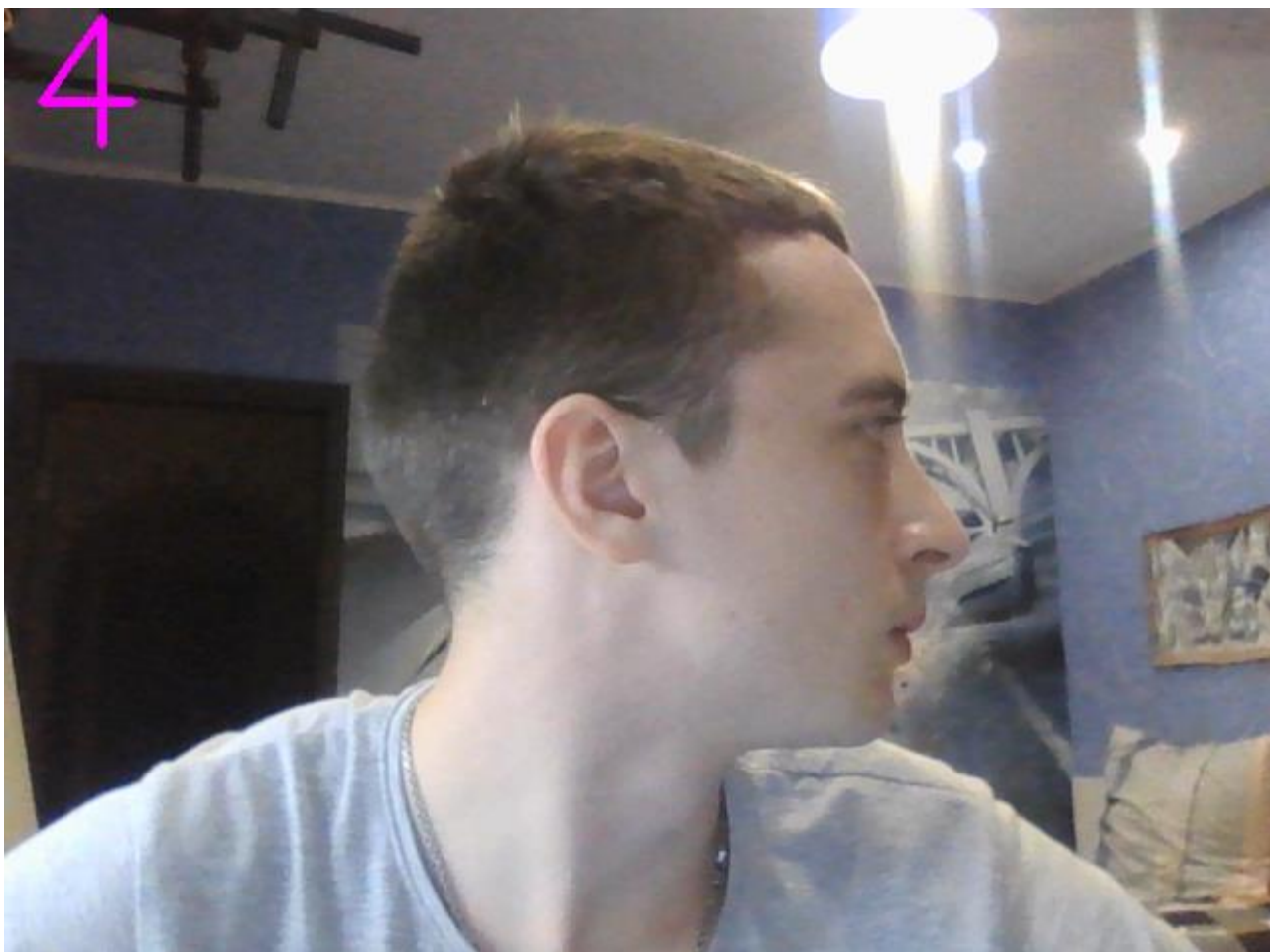


Рисунок 4.6 – Зображення з відеокамери експерименту №3 для алгоритмів бібліотеки Face-recognition

Для рисунку 4.5 та 4.6 було отримано дані, що зведено у таблиці 4.3:

Таблиця 4.3 Використання системою ресурсів під час експерименту №3

	Алгоритми бібліотеки MTCNN	Алгоритми бібліотеки Face-recognition	Різниця
Час виявлення обличчя, с	0.79	Не може виявити обличчя в подібних умовах	Порівняння не можливе
Використання RAM, мб	775.04		
Використання ресурсів процесора, %	19.5		

Умови проведення експерименту №4 будуть наступні:

- рівень освітлення: достатній, наявне сонячне освітлення та додаткове освітлення ламп в кімнаті;
- час доби: 14.00;
- кут обличчя до камери: фронтальне зображення;
- перешкоди між камерою та обличчям: окуляри;
- дистанція до камери: 60 см.

Зображення з відеокамери продемонстроване на рисунку 4.7, 4.8:

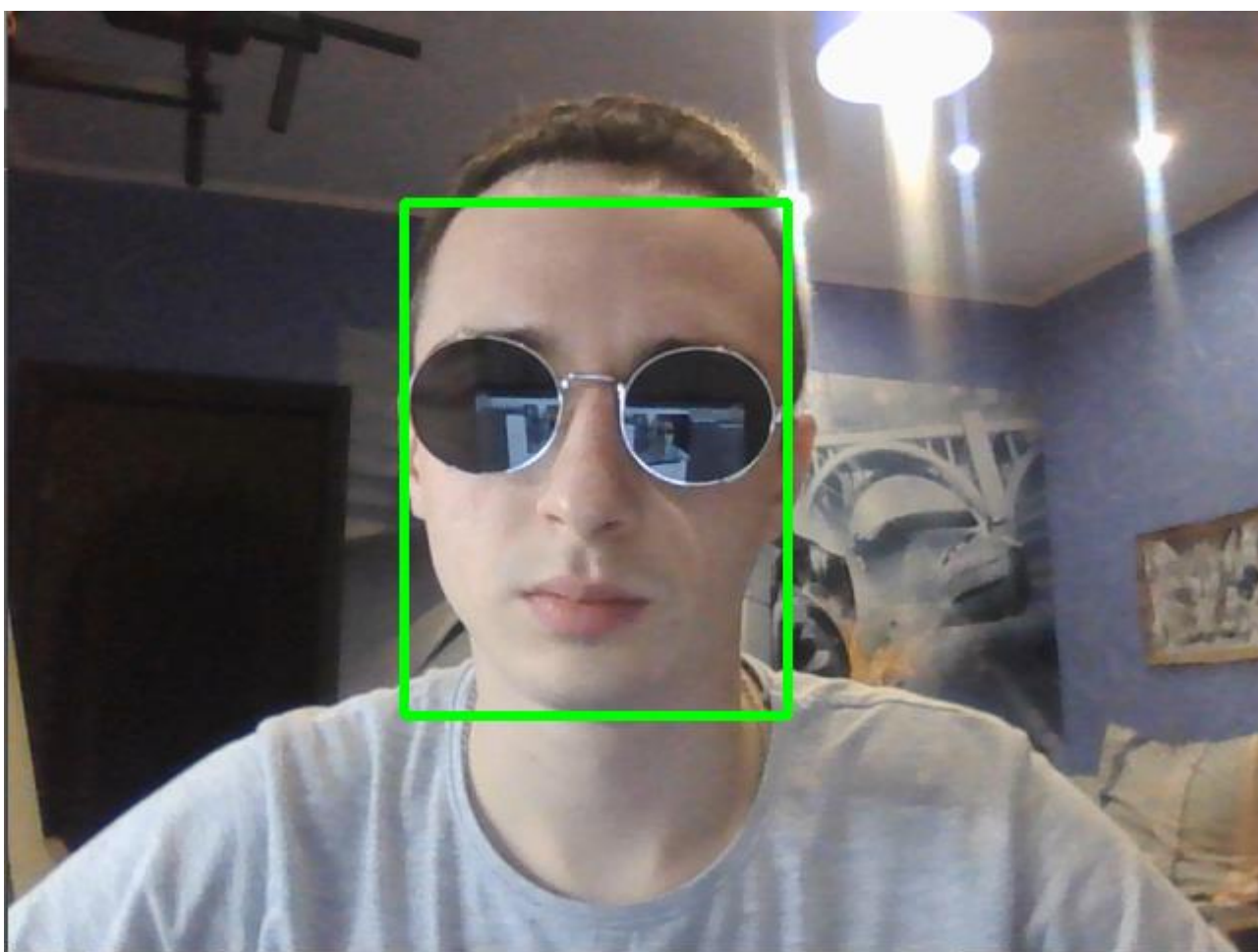


Рисунок 4.7 – Зображення з відеокамери експерименту №4 для алгоритмів бібліотеки
MTCNN

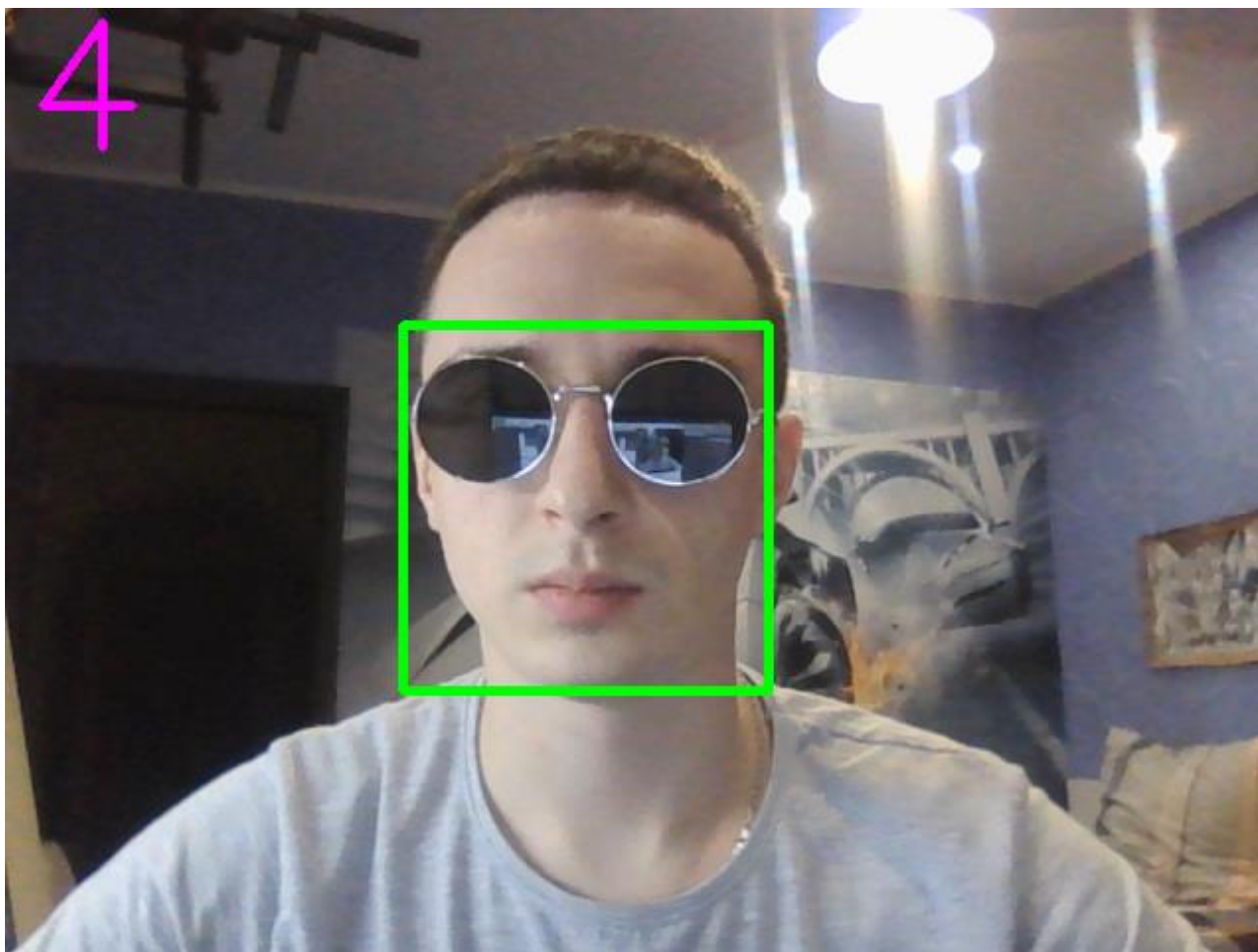


Рисунок 4.8 – Зображення з відеокамери експерименту №4 для алгоритмів бібліотеки Face-recognition

Для рисунку 4.7 та 4.8 було отримано дані, що зведено у таблиці 4.4:

Таблиця 4.4 Використання системою ресурсів під час експерименту №4

	Алгоритми бібліотеки MTCNN	Алгоритми бібліотеки Face-recognition	Різниця
Час виявлення обличчя, с	0.79	0.195	0.595
Використання RAM, мб	521.17	465.05	56.12
Використання ресурсів процесора, %	19.3	12.5	6.8

Умови проведення експеременту №5 будуть наступні:

- рівень освітлення: достатній, наявне сонячне освітлення та додаткове освітлення ламп в кімнаті;
- час доби: 14.00;
- кут обличчя до камери: фронтальне зображення;
- перешкоди між камерою та обличчям: відсутні;
- дистанція до камери: 140 см.

Зображення з відеокамери продемонстроване на рисунку 4.9, 4.10:

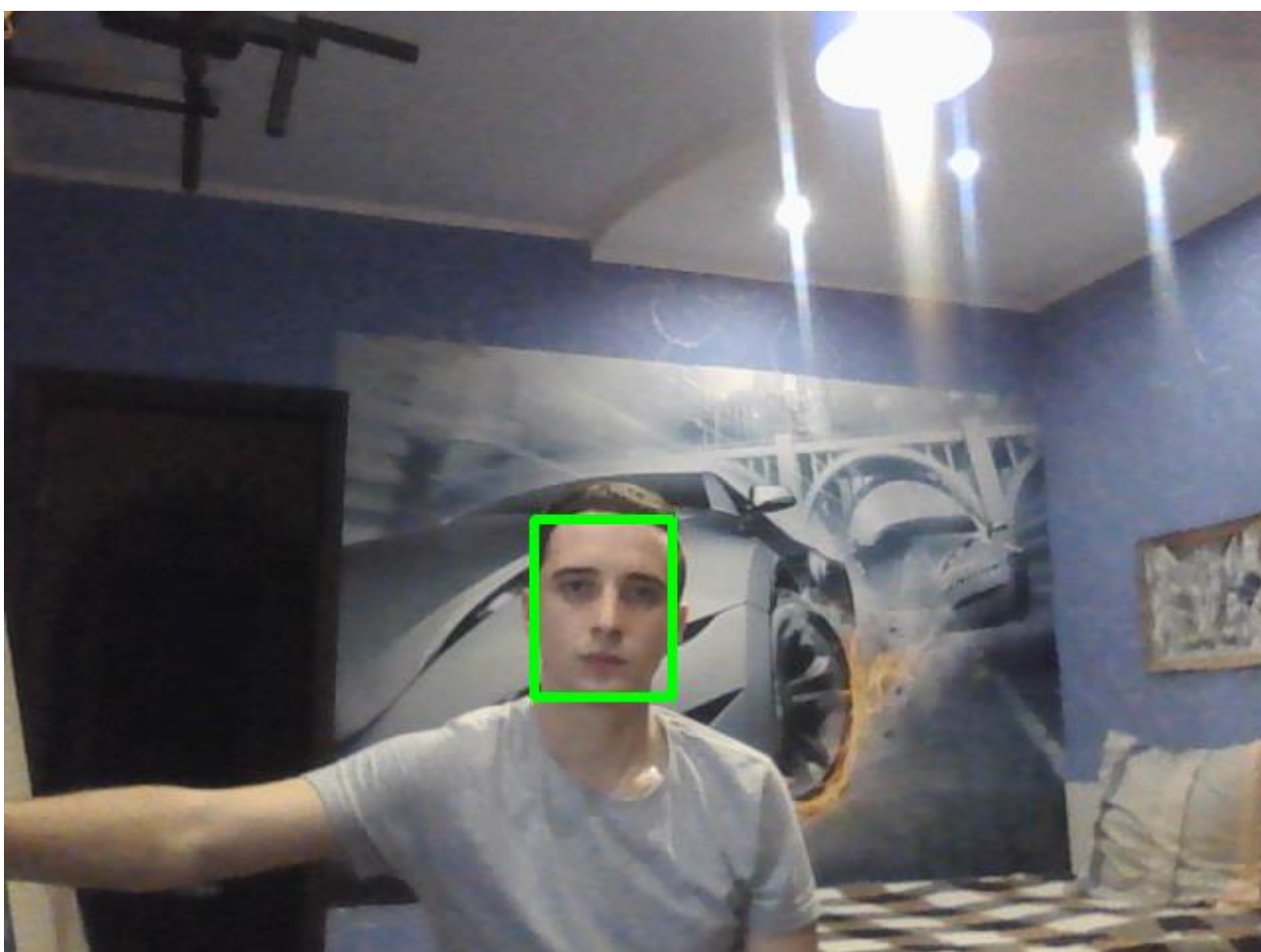


Рисунок 4.9 – Зображення з відеокамери експеременту №5 для алгоритмів бібліотеки
MTCNN

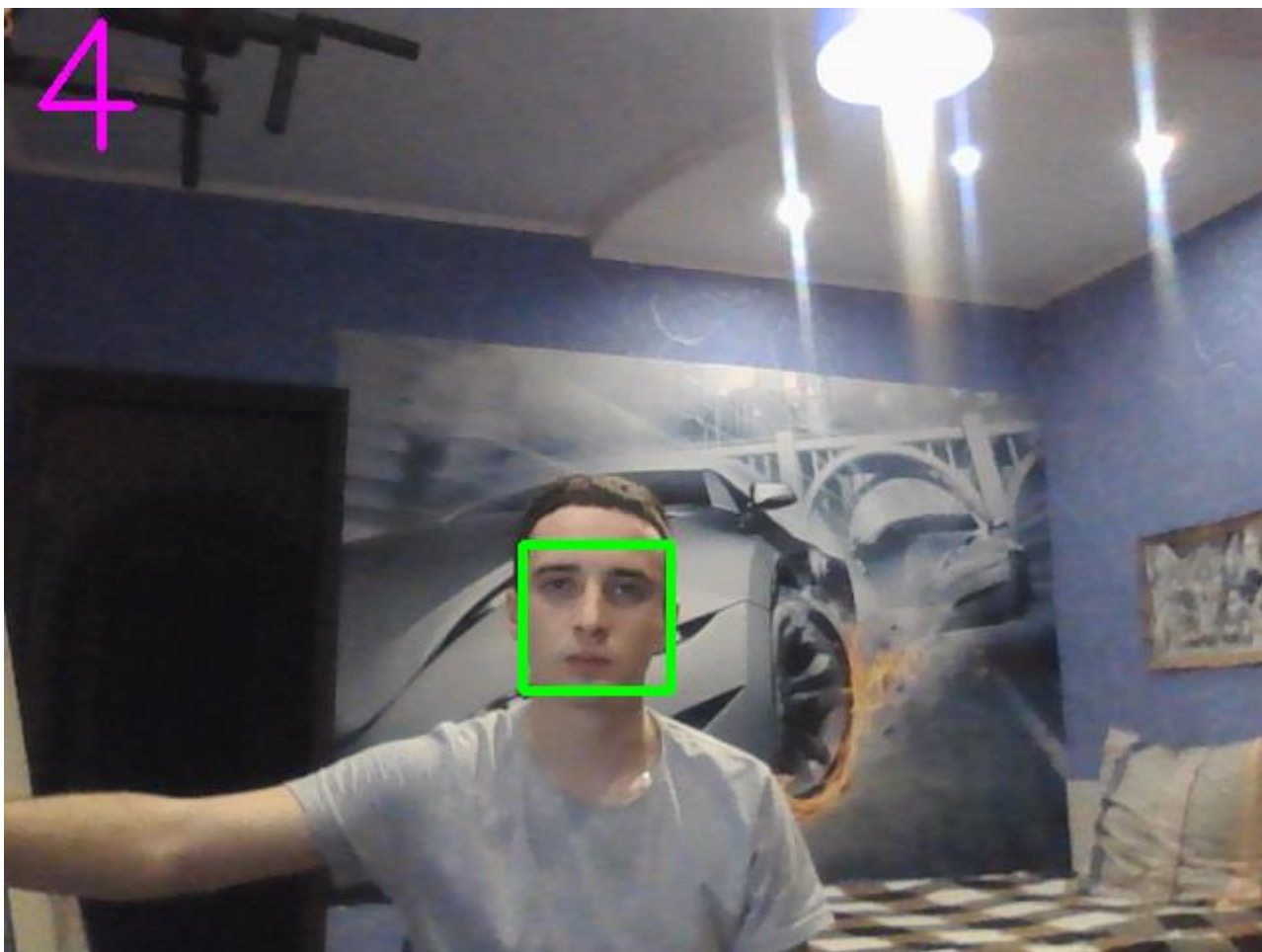


Рисунок 4.10 – Зображення з відеокамери експерименту №5 для алгоритмів бібліотеки Face-recognition

Для рисунку 4.9 та 4.10 було отримано дані, що зведено у таблиці 4.5:

Таблиця 4.5 Використання системою ресурсів під час експерименту №5

	Алгоритми бібліотеки MTCNN	Алгоритми бібліотеки Face-recognition	Різниця
Час виявлення обличчя, с	0.77	0.193	0.577
Використання RAM, мб	548.92	465.24	82,68
Використання ресурсів процесора, %	16.6	12.4	4.2

Для визначення точності (Accuracy) та F-міри потрібно провести більшу кількість експериментів. Впродовж дня з інтервалом в 15хв. було зроблено по 30 спроб розпізнавання обличчя для кожної бібліотеки. Результати експерименту для бібліотеки Face-recognition відображені у таблиці 4.6:

Таблиця 4.6 Матриця помилок для експериментів з бібліотекою Face-recognition

Face-recognition	Accept	Reject
Reject	2 Type 1 error (False accept)	2 Correct (True reject)
Accept	21 Correct (True accept)	5 Type 2 error (False reject)

Таким чином можна визначити точність та повноту:

$$\text{Влучність}_{FR} = \frac{21}{23} = 0.913$$

$$\text{Повнота}_{FR} = \frac{21}{26} = 0.807$$

Тоді традиційна F-міра, або збалансована F-оцінка, що є середнім гармонійним точності та повноти буде дорівнювати:

$$F_1 = \frac{2}{\text{повнота}^{-1} + \text{влучність}^{-1}} = 2 * \frac{\text{влучність} * \text{повнота}}{\text{влучність} + \text{повнота}} = 2 * \frac{0.736}{1.72} = 0.85$$

Тепер визначимо точність розпізнавання:

$$\text{Точність} = \frac{21}{30} = 0.7$$

Результати експерименту для бібліотеки MTCNN відображені у таблиці 4.7:

Таблиця 4.7 Матриця помилок для експериментів з бібліотекою MTCNN

Face-recognition	Accept	Reject
Reject	3 Type 1 error (False accept)	1 Correct (True reject)
Accept	25 Correct (True accept)	1 Type 2 error (False reject)

$$\text{Влучність}_{MTCNN} = \frac{25}{28} = 0.89$$

$$\text{Повнота}_{MTCNN} = \frac{25}{26} = 0.96$$

Тоді традиційна F-міра, або збалансована F-оцінка, що є середнім гармонійним точності та повноти буде дорівнювати:

$$F_1 = \frac{2}{\text{повнота}^{-1} + \text{влучність}^{-1}} = 2 * \frac{\text{влучність} * \text{повнота}}{\text{влучність} + \text{повнота}} = 2 * \frac{0.85}{1.85} = 0.91$$

Тепер визначимо точність розпізнавання:

$$\text{Точність} = \frac{25}{30} = 0.83$$

4.2 Аналіз результатів експериментів

Робота алгоритмів у реальному часі. За результатами експериментальних даних стосовно часу виявлення обличчя, які були отримані під час роботи розробленої системи можна стверджувати, що час, затрачений на роботу алгоритмів виявлення обличчя методами бібліотеки MTCNN, набагато більший ніж у методів бібліотеки Face-recognition. При цьому, різниця в часі розпізнавання $0,688 > \Delta_t > 0,577$. Для роботи алгоритмів розпізнавання при зменшенні освітлення потрібно витратити трохи більше часу для процесу виявлення, ніж при наявності перешкод на обличчі або зміні дистанції до обличчя. До того ж, потрібно зазначити, що під час експерименту №3 для роботи алгоритмів бібліотеки Face-recognition не вдалось встановити потрібні дані тому, що методи бібліотеки не змогли виявити обличчя, яке знаходиться під кутом 90 градусів до камери. Для наочності діаграма порівняння часу виявлення обличчя представлена на рисунку 4.11:

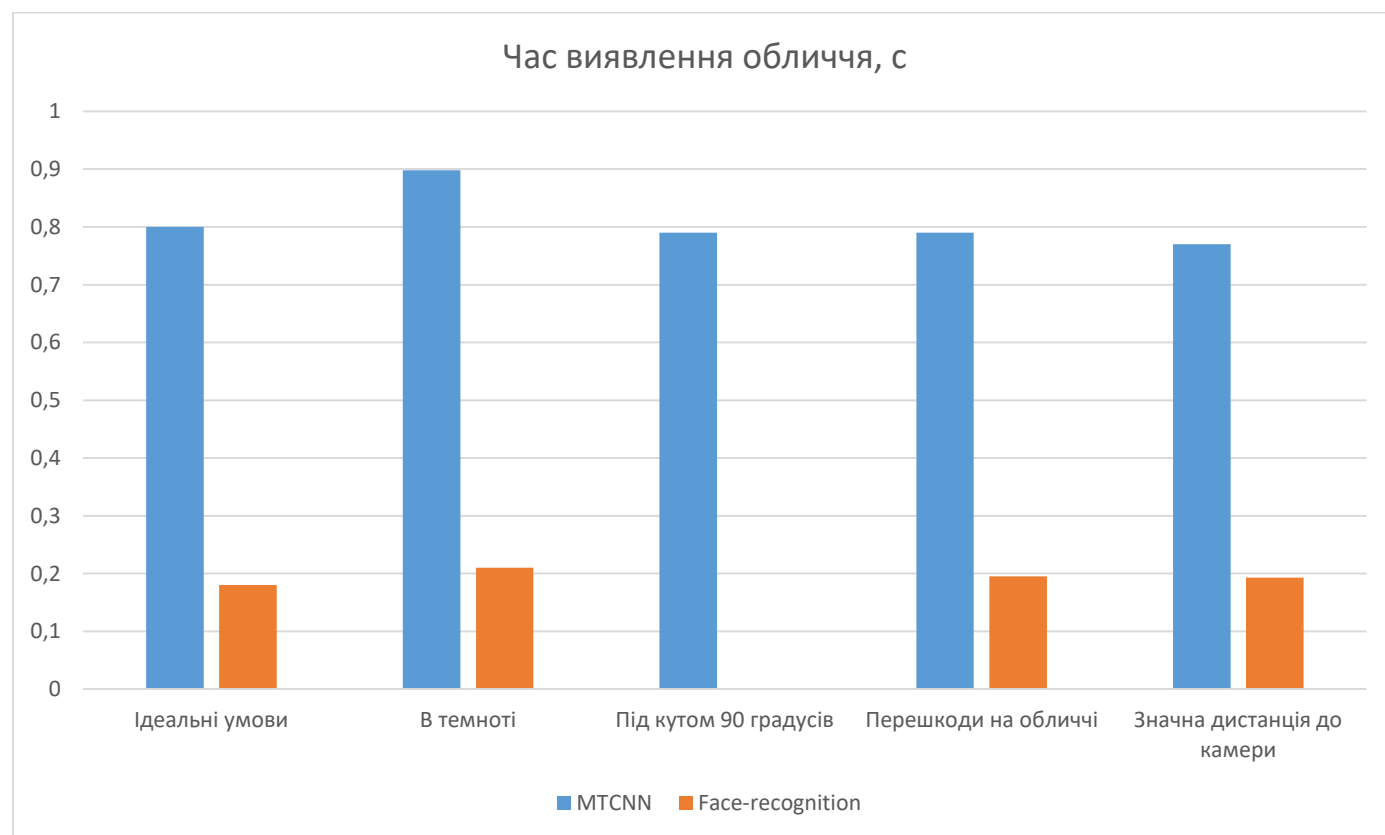


Рисунок 4.11 – Діаграма для порівняння часу виявлення обличчя алгоритмами бібліотек MTCNN та Face-recognition

Використання ресурсів оперативної пам'яті. За результатами експериментальних даних стосовно використання оперативної пам'яті, які були отримані під час роботи розробленої системи можна стверджувати, що обсяг оперативної пам'яті, затрачений на роботу алгоритмів виявлення обличчя методами бібліотеки MTCNN, дещо більший ніж у методів бібліотеки Face-recognition. При цьому, різниця в обсязі використання оперативної пам'яті $82,68 > \Delta_{RAM} > 51,08$. Для роботи алгоритмів розпізнавання бібліотеки MTCNN при повороті обличчя під кутом 90 градусів необхідно було використати значно більше оперативної пам'яті, ніж при виконанні інших експериментів. До того ж, потрібно зазначити, що під час експерименту №3 для роботи алгоритмів бібліотеки Face-recognition не вдалось встановити потрібні дані тому, що методи бібліотеки не змогли виявити обличчя, яке знаходиться під кутом 90 градусів до камери. Для наочності діаграма порівняння використання оперативної пам'яті представлена на рисунку 4.12:

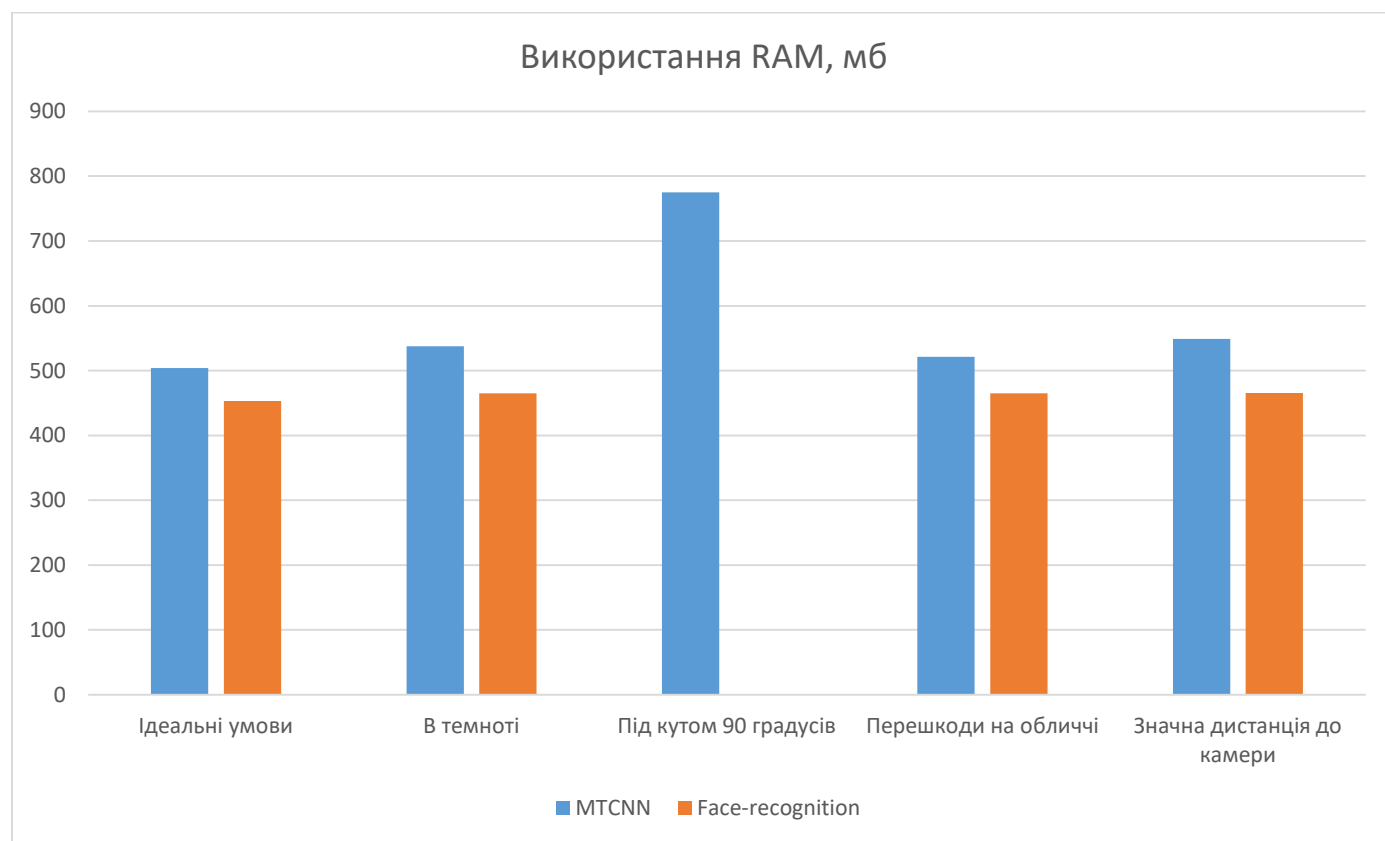


Рисунок 4.12 – Діаграма для порівняння використання оперативної пам'яті алгоритмами бібліотек MTCNN та Face-recognition

Використання ресурсів процесора. За результатами експериментальних даних стосовно використання ресурсів процесора, які були отримані під час роботи розробленої системи можна стверджувати, що обсяг використання ресурсів процесора, затрачений на роботу алгоритмів виявлення обличчя методами бібліотеки MTCNN, більший ніж у методів бібліотеки Face-recognition. При цьому, різниця в обсязі використання ресурсів процесора $6,8 > \Delta_{CPU} > 4,2$. Для роботи алгоритмів розпізнавання бібліотеки MTCNN при повороті обличчя під кутом 90 градусів та за наявності перешкод на обличчі необхідно було використати більше ресурсів процесора, ніж при виконанні інших експериментів. До того ж, потрібно зазначити, що під час експерименту №3 для роботи алгоритмів бібліотеки Face-recognition не вдалось встановити потрібні дані тому, що методи бібліотеки не змогли виявити обличчя, яке знаходиться під кутом 90 градусів до камери. Для наочності діаграма порівняння використання ресурсів процесора представлена на рисунку 4.13:

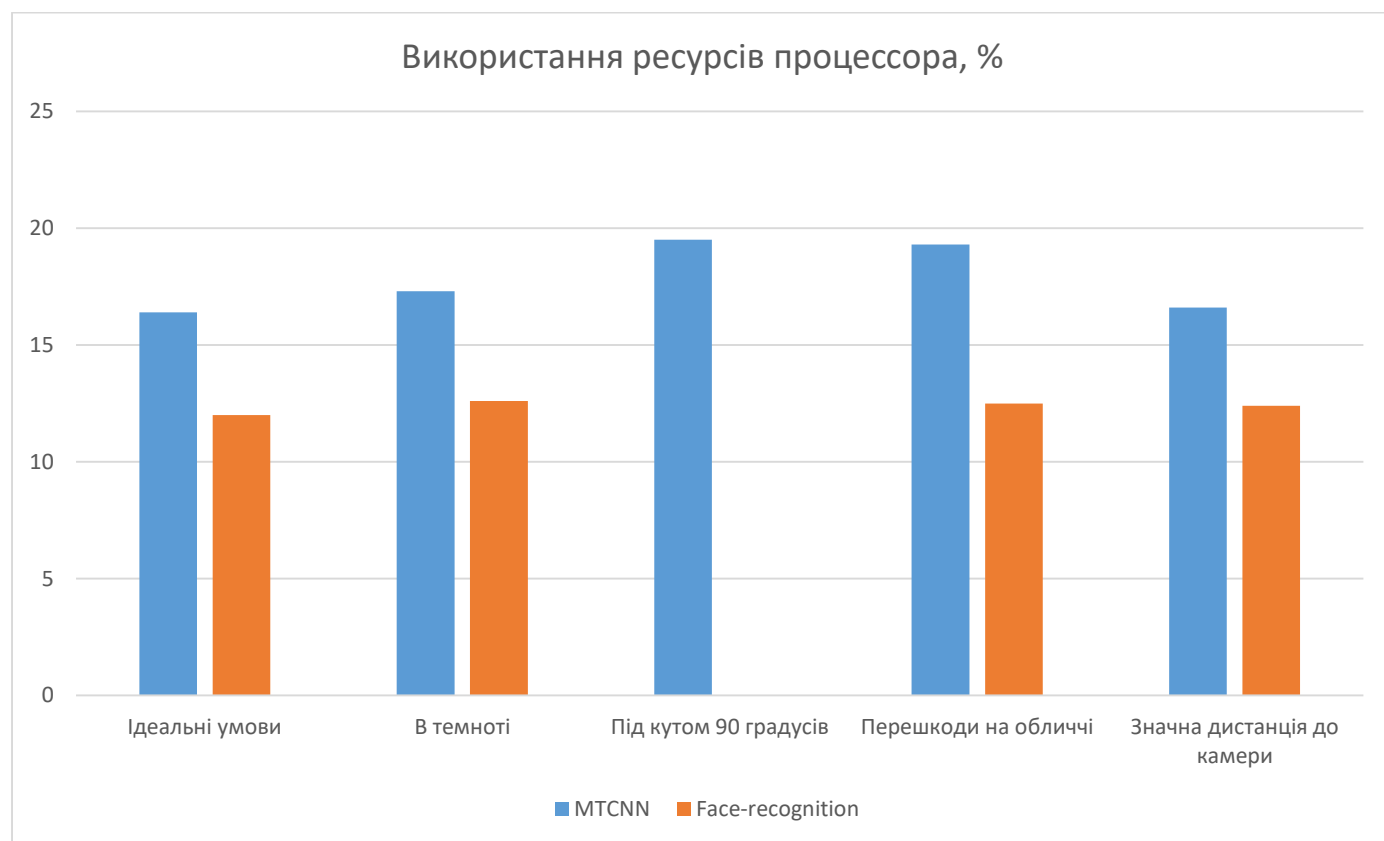


Рисунок 4.13 – Діаграма для порівняння використання ресурсів процесора алгоритмами бібліотек MTCNN та Face-recognition

Збалансована оцінка F-міра досягає свого найкращого значення при 1, а найгіршого при 0. Під час дослідження ефективності алгоритмів бібліотек розпізнавання обличчя F-міра використана для оцінки здатності системи розпізнавання точно визначати обличчя і уникати неправильних визначень. За результатами експериментальних даних можна побачити, що F-міра для алгоритмів бібліотеки MTCNN дещо більша, ніж у алгоритмів бібліотеки Face-recognition, а це означає, що визначення обличчя в різних умовах навколишнього середовища алгоритмами бібліотеки MTCNN покриває більше виняткових ситуацій, коли немає фронтального зображення обличчя людини. Для наочності діаграма порівняння метрик ефективності алгоритмів представлена на рисунку 4.14:

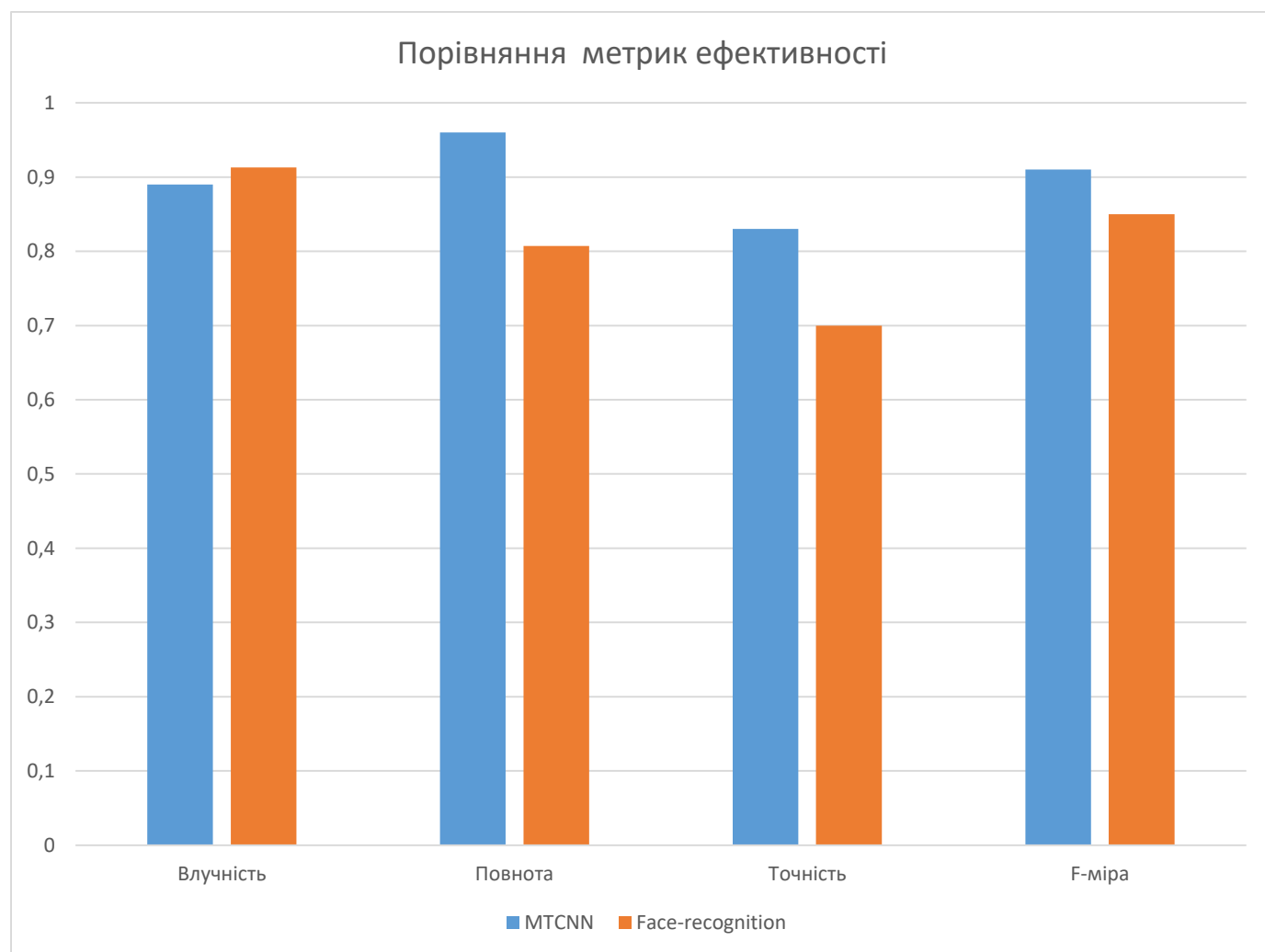


Рисунок 4.14 – Діаграма для порівняння метрик ефективності алгоритмів бібліотек MTCNN та Face-recognition

На основі вищеописаних результатів експериментів можемо зробити висновки про зручність використання бібліотек мови Python MTCNN та Face-recognition:

Основні переваги у зручності використання бібліотеки MTCNN:

- висока точність виявлення. MTCNN визначає обличчя та ключові точки з високою точністю, що робить його ефективним для завдань розпізнавання обличчя;
- широкі можливості виявлення. MTCNN виявляє обличчя, очі та рот, що дозволяє використовувати його для багатьох завдань в реальному часі;
- використання у нестандартних умовах навколишнього середовища. Алгоритми бібліотеки пристосовані виявляти обличчя у різних складних умовах навколишнього середовища.

Основні переваги у зручності використання бібліотеки Face-recognition:

- зручна ідентифікація. Алгоритми бібліотеки можна легко використовувати для ідентифікації осіб, що робить їх корисними для сценаріїв співставлення людей для авторизації;
- добре документована. Бібліотека має добре організовану та зрозумілу документацію, що спрощує процес вивчення та використання;
- швидкодія роботи для виявлення обличчя. Алгоритми бібліотеки добре пристосовані для виявлення позиції фронтального зображення обличчя в цілому.

Висновки до четвертого розділу

Проведено експериментальні дослідження системи. Результати експериментів занесено до відповідних таблиць. Проведено порівняння результатів, яке відображено для наочності у діаграмах. Надано оцінку отриманим даним, сформовано висновок, щодо використання бібліотек у розробці систем розпізнавання обличчя у режимі реального часу.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

На основі проведеної роботи можна стверджувати, що використання систем розпізнавання обличчя у режимі реального часу за період свого розвитку досягло чималих успіхів. Подібні системи застосовуються в тому чи іншому вигляді для вирішення великої кількості задач у сферах суспільства – від високотехнологічних аеропортів до торгових центрів. Новаторські технології розпізнавання обличчя стали не лише засобом забезпечення безпеки, а й інструментом для вирішення широкого спектру завдань у суспільстві.

Однак, варто визнати, що найсучасніші системи розпізнавання дають задовільну продуктивність лише за контрольованих сценаріїв. Точність розпізнавання значно погіршується, коли стикається з необмеженою ситуацією. Відносно нещодавно дослідники почали проводити експерименти розпізнавання обличчя у необмежених умовах для визначення факторів, що впливають на ефективність таких систем. Реалізовані системи все ще стикаються з проблемами під час розпізнавання, хоча й їх ефективність значно покращилась за період вивчення дослідниками цієї сфери. Вирішення цих проблем вимагатиме подальших технологічних вдосконалень та досліджень в галузі машинного навчання та комп'ютерного зору. Створення більш адаптованих та стійких до змін навколишнього середовища систем та проведені експерименти дослідження ефективності алгоритмів розпізнавання бібліотек MTCNN та Face-recognition на основі запропонованих метрик дозволять у майбутньому впевнено стверджувати про великий стрибок у розвитку сфери розпізнавання обличчя у режимі реального часу.

Опорою для майбутніх досліджень може стати створена система, яка має розроблену структуру проекту, чітко визначені функції та області відповідальності, демонструє відмінну відповідність початковим вимогам та має можливість масштабування для розширення функціональності шляхом вдосконалення для проведення експериментальних досліджень.

В результаті виконаної роботи можна сказати, що рекомендується робити вибір між бібліотеками та їх можливостями в залежності від системи, для якої розробляється процедура аутентифікації користувача. У випадках створення системи, що працює в ідеальних умовах, можна надати перевагу бібліотеці Face-recognition, яка використовує глибокі нейронні мережі для витягування векторів обличчя, має лаконічний API та методи визначення і порівняння векторів обличчя для ідентифікації, тоді як бібліотека MTCNN використовує каскадні класифікатори лише для виявлення обличчя, визначає ключові точки з високою точністю навіть в досить поганих умовах навколишнього середовища, але не надає функціональності для порівняння обличчя, що примушує використовувати її як частину більш масштабних систем розпізнавання обличчя.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Книги	
Один автор	1. Harry Wechsler, Reliable Face Recognition Methods, 2007
Два автори	1. Mark Andrejevic, Neil Selwyn. Facial Recognition, 2022 2. Anil K. Jain, Stan Z. Li, Handbook of Face Recognition, 2016
Три автори	1. S. Kevin Zhou, Rama Chellappa, Wenyi Zhao, Unconstrained Face Recognition, 2006
Стандарти	1. ДСТУ 8302:2015. Інформація та документація. БІБЛІОГРАФІЧНЕ ПОСИЛАННЯ. Загальні положення та правила складання, від 22 червня 2015 р. № 61 з 2016-07-01; згідно з наказом ДП «УкрНДНЦ» від 04 березня 2016 р. № 65 змінено дату чинності. Київ ДП «УкрНДНЦ» 2016. 16 с. 2. ПОЛОЖЕННЯ ПРО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИВ УКРАЇНСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ НАУКИ І ТЕХНОЛОГІЙ, протокол №5 від 28.03.2022; згідно з наказом УДУНТ від 07.04.22 №27, Дніпро 2022
Електронні ресурси	
Статті з періодичних видань	[2] 1. Z. Rybchak, O. Basystiuk. Analysis of computer vision and image analysis technics. ECONTECHMOD. AN INTERNATIONAL QUARTERLY JOURNAL, 2017. Vol. 6. No. 2. 79–84. URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/fef6bb85-9d4c-4077-82a6-d30d60432517/content [3] 2. ГОЛУБ'ЯК І.В., КОСАРЕВИЧ Р.Я. МЕТОДИ РОЗПІЗНАВАННЯ ОБЛИЧ. ПРОБЛЕМИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, 2017. С. 158-164. URL: https://core.ac.uk/download/pdf/234094400.pdf [4] 3. Ю. А. Тимошин, С. П. Орленко. АЛГОРИТМ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДЕЙ НА БАЗІ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ.

	Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 1' (32) 2018. С. 166-173. URL: https://ela.kpi.ua/bitstream/123456789/34277/1/asau-2018-1_19.pdf [5] 4. P. Viola, M. Jones. Rapid Object Detection using a Boosted Cascade of Simple Features. ACCEPTED CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION 2001. URL: https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf 5. P. Viola, M. Jones. Robust real-time face detection. International Journal of Computer Vision, vol. 57, no. 2, 2004., pp.137–154
Сторінки з веб-сайтів	[6] 1. FacePay24 спосіб оплати: веб-сайт. URL: https://privatbank.ua/facepay24 [7] 2. СПОСОБИ ЗІСТАВЛЕННЯ ОСОБИ З ЇЇ ФОТОЗОБРАЖЕННЯМ. URL: https://center.diia.gov.ua/uploads/0/1003-brosura.pdf [8] 3. Система розпізнавання облич Clearview AI: веб-сайт. URL: https://www.ukrinform.ua/rubric-technology/3694894-zavdaki-programi-rozpiznavanna-oblic-vstanovili-osobi-10-tisac-rosijskih-voennih-zlocinciv.html [9] 4. Використання системи розпізнавання обличчя в Україні: веб-сайт. URL: https://ms.detector.media/withoutsection/post/32053/2023-05-26-vykorystannya-systemy-rozpiznavannya-oblychchya-v-ukraini-zakonodavcho-ne-vregulovano-pravozakhysnyk/ [10] 5. Система розпізнавання облич: веб-сайт. URL: https://uk.wikipedia.org/wiki/Система_розпізнавання_облич#P”PsPrP°С,PsPє [11] 6. Face Recognition 1.3.0: веб-сайт. URL: https://pypi.org/project/face-recognition/ [12] 7. Mtcnn 0.1.1: веб-сайт. URL: https://pypi.org/project/mtcnn/

	[13] 8. Матриця невідповідностей: веб-сайт. URL: https://uk.wikipedia.org/wiki/Матриця_невідповідностей [14] 9. F-міра: веб-сайт. URL: https://uk.wikipedia.org/wiki/F-міра [15] 10. Проектування інтерфейсу користувача: веб-сайт. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/1415/2/Rozdil1.pdf
Частина видання	
Тези доповідей, матеріали конференції	[1] 1. Різниченко М. О., Горбова О. В. Дослідження методів та засобів аутентифікації користувача у реальному часі шляхом розпізнавання обличчя: матеріал XVII міжнародної науково-практичної конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» (Дніпро, УДУНТ, 13-14 грудня 2023 року). С. 89

ДОДАТКИ