

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)
Моделі ідентифікації особистості за біометричними ознаками
(тема)

Виконав: студент 2 курсу, групи СКСм-21-1
Сіленко М.С.

(прізвище, ініціали)

Спеціальність 123 Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Спеціалізовані комп'ютерні системи
(повна назва освітньої програми)

Керівник роботи доц. Шкіль О.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри


(підпис)

Чумаченко С.В.
(прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет _____ Комп'ютерної інженерії та управління _____

Кафедра _____ Автоматизації проектування обчислювальної техніки _____

Рівень вищої освіти _____ другий (магістерський) _____

Спеціальність _____ 123 Комп'ютерна інженерія _____
(шифр і назва)

Тип програми _____ Освітньо-професійна _____
(освітньо-професійна або освітньо-наукова)

Освітня програма _____ Спеціалізовані комп'ютерні системи _____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____ 

(підпис)

«02» 09 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові _____ Сіленку Максиму Сергійовичу _____
(прізвище, ім'я, по батькові)

1. Тема роботи _____ Моделі ідентифікації особистості за біометричними ознаками _____

затверджена наказом по університету від 14 11 2022 р. № 1478 Ст _____

2. Термін подання студентом роботи до екзаменаційної комісії 12.12.2022 р.

3. Вихідні дані до роботи 1) спосіб ідентифікації: ідентифікація особи за біометричними характеристиками;

2) біометричні характеристики: обличчя, відбиток пальця, райдужна оболонка ока;

3) мова програмування: Python;

4) середовище: PyCharm

4. Перелік питань, що потрібно опрацювати в роботі _____

1) аналіз проблеми;

2) огляд існуючих методів ідентифікації за обличчям;

3) огляд існуючих методів ідентифікації за відбитком пальця;

4) огляд існуючих методів ідентифікації за райдужною оболонкою ока;

5) вибір технології розробки та інструментальних засобів;

6) удосконалення існуючих алгоритмів;

7) висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____
Слайд-презентація – 22 слайди

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

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

7. Дата видачі завдання 01.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз проблеми	01.09.22-20.09.22	
2	Огляд існуючих методів ідентифікації за обличчям	21.09.22-01.10.22	
3	Огляд існуючих методів ідентифікації за відбитком пальця	02.10.22-15.10.22	
4	Огляд існуючих методів ідентифікації за райдужною оболонкою ока	16.10.22-25.10.22	
5	Вибір технології розробки та інструментальних засобів	26.10.22-02.11.22	
6	Удосконалення існуючих алгоритмів	03.11.22-17.11.22	
7	Оформлення матеріалів кваліфікаційної роботи	18.11.22-04.12.22	
8	Подання кваліфікаційної роботи керівникові	05.12.22-15.12.22	
9	Представлення роботи до захисту	05.12.22-22.12.22	

Студент  _____
 (підпис)

Керівник роботи  _____ доц., к.т.н Шкіль О.С
 (підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи містить 59 сторінок, 12 рисунків, 7 таблиць, 3 лістинга та 7 джерел за переліком посилань.

ІДЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ СИСТЕМИ, БІОМЕТРИЧНІ ХАРАКТЕРИСТИКИ, БЕЗПЕКА, ОЗНАКИ ОБЛИЧЧЯ, АЛГОРИТМИ, ВІДБИТОК ПАЛЬЦЯ, РАЙДУЖНА ОБОЛОНКА ОКА

Метою кваліфікаційної роботи є дослідження та модифікація алгоритмів біометричної ідентифікації для підвищення їх показників швидкодії та точності розпізнавання, методами об'єднання певних алгоритмів, а також використанням технологій ML. Даний вид роботи сприяє поглибленому аналізу та вивченню методів біометричної ідентифікації особистості.

В рамках роботи описано основні етапи процесу ідентифікації, відмінність від верифікації, а також методи та алгоритми роботи з біометричними характеристиками, які використовуються сьогодні.

ABSTRACT

The explanatory note contains: 59 pages, 12 figures, 7 tables, 3 listings and 7 sources according to the list of links.

IDENTIFICATION, BIOMETRIC SYSTEMS, BIOMETRIC CHARACTERISTICS, SECURITY, FACIAL SIGNS, ALGORITHMS, FINGER PRINT, IRIS

The purpose of the work is discovering and modification of biometric identification algorithms to increase their speed and recognition accuracy, using methods of combining certain algorithms, as well as using ML technologies. This type of work contributes to the in-depth analysis and study of biometric identification methods.

This work describes the main stages of the identification process, the difference from verification, as well as methods and algorithms for working with biometric characteristics that are used today.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП	9
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ.....	11
1.1 Загальне визначення біометричних систем	11
1.2 Різновиди біометричних ознак	12
1.3 Основи поняття ідентифікації	13
1.4 Постановка задачі дослідження	15
2 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ	18
2.1 Метод Хаар характеристик	18
2.2 Метод власних обличч (Eigenfaces)	24
2.3 Удосконалення алгоритму ідентифікації обличчя.....	27
3 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ВІДБИТКУ ПАЛЬЦЯ.....	30
3.1 Загальні положення про ідентифікацію за відбитком пальця	30
3.2 Удосконалення алгоритму ідентифікації за відбитком пальця	34
4 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОКА.....	38
4.1 Загальні положення про ідентифікацію ока.....	38
4.2 Ідентифікація особистості за райдужною оболонкою.....	42
4.3 Алгоритми знаходження шаблону райдужної оболонки.....	46
4.4 Методи порівняння шаблонів райдужної оболонки.....	48
4.5 Удосконалення алгоритму ідентифікації за оком.....	50
5 ВИБІР ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РЕАЛІЗАЦІЇ.....	55
4.1 Огляд технологій.....	55
4.2 Мова програмування Python.....	55
4.3 Бібліотека OpenCV.....	56
ВИСНОВКИ	58
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ	59

ДОДАТОК А Графічний матеріал кваліфікаційної роботи.....	60
ДОДАТОК Б Імплементація модифікованих алгоритмів.....	71
Б.1 Лістинг алгоритму розпізнавання обличчя.....	71
Б.2 Лістинг модифікованого алгоритму ідентифікації за оком.....	71
Б.3 Лістинг етапу нормалізації алгоритму ідентифікації за відбитком пальця	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

LBPН - алгоритм узагальнює локальну структуру зображення, порівнюючи кожен піксель із сусідами, і результат перетворюється у двійкове число (англ., Local Binary Patterns Histogram)

PCA - Principal Component Analysis

АЦП - аналого-цифровий перетворювач

AFIS - Automated Fingerprint Identification System

OS - Operation System

ВСТУП

На сьогоднішній день все швидше відбувається розвиток цифрових технологій, до яких належать нові види ідентифікації особистості у різних сферах, а одним із найефективніших методів перевірки особистості є біометрична ідентифікація, що свідчить про актуальність даної роботи.

Біометричні характеристики у сукупності є повністю унікальним ідентифікатором для кожної особи. Такі дані не можуть бути скопійованими або переданими третім особам, що в свою чергу знову свідчить про їх надійність. Ще одним позитивним фактором такого способу ідентифікації є комфортні умови використання таких даних, тому що людині не потрібно створювати та запам'ятовувати складний пароль, щоб його не зламали, або постійно пам'ятати та носити із собою ключ-карту чи перейматися про надійність сховища ваших паролів, біометричні данні даються людині від народження та постійно при ній.

Захист приватних даних та особиста безпека завжди були, є та залишатимуться актуальними темами для суспільства, адже кожен хоче відчувати себе захищеним. Корпорації завжди переймаються що інформація повністю захищена та доступ мають тільки довірені особи. Органи влади, що відповідають за дотримання правопорядку постійно контролюють рівень загрози у публічних місцях та під час масових заходів, щоб гарантувати громадянам безпеку. Навіть кожна звичайна людина думає про те, як захистити свою власність та запобігти вторгненню зловмисників.

Досягнення вказаних цілей дозволить більш активно використовувати біометричні ознаки для розпізнання особистості, популяризувати дані моделі ідентифікації, відкрити нові можливості у сфері технологій, а також розширити межі застосування в інших сферах. Наприклад захист мобільних девайсів та персональних комп'ютерів, шифрування інформації, підтвердження особи для потрапляння на територію, що охороняється.

Правоохоронні органи легко зможуть ідентифікувати зловмисників за їх біометричними даними. Використання таких систем у аеропортах, вокзалах чи інших людних місцях прискорить пошук людини в натовпі, за рахунок роботи в режимі реального часу.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Загальне визначення біометричних систем

Біометричні системи – це системи, які використовують анатомічні та поведінкові характеристики, які називаються біометричними ознаками, для автоматичного розпізнавання людей. Використання таких характеристик стає важливим у рішеннях для ідентифікації особи, оскільки вони відображають фізичну ідентичність особи і не можуть бути ні розповсюджені, ні втрачені. Слово біометрика походить від грецьких слів *bios* (що означає життя) і *metron* (означає вимірювання), тому біометричні ознаки — це вимірювання живого людського тіла. За допомогою слова реєстрація ми визначаємо акт захоплення біометричної характеристики за допомогою біометричного датчика (наприклад, сканера відбитків пальців), створення компактного, але виразного представлення інформації (набір функцій) і, нарешті, організацію однієї або кількох ознак. встановлює шаблон реєстрації, який буде збережено в якомусь постійному сховищі. Біометрична система може бути системою верифікації або системою ідентифікації.

Система верифікації підтверджує особистість особи, порівнюючи отриману біометричну ознаку з зареєстрованою. Проводиться порівняння один до одного, щоб підтвердити є особа тим, за кого себе видає. Ця система приймає або відхиляє подану заяву про ідентифікацію.

Система ідентифікації розпізнає особу, шукаючи в базі даних відповідність із раніше захопленим (зареєстрованим) шаблоном біометричного посилання. Він проводить порівняння один до багатьох, щоб визначити, чи є особа в базі даних чи ні, і якщо так, вона повертає ідентифікатор посилання на реєстрацію, який відповідає.

1.2 Різновиди біометричних ознак

Біометричні системи можуть працювати з різними біометричними ознаками, які притаманні людині. Нижче наведено короткий перелік найбільш поширених біометричних ознак.

Відбиток пальця. Це біометрична ознака з найбільш бажаними властивостями. Насправді кожна людина має пальці, а отже, і відбитки пальців. Вони дуже характерні та постійні; навіть якщо вони тимчасово незначно змінюються через порізи та синці на шкірі, відбиток пальця знову з'являється після загоєння пальця. Сканери відбитків пальців із живим скануванням можуть легко знімати високоякісні зображення відбитків пальців, просто прикладаючи палець до датчика. Відбитки пальців мають довгу історію використання в криміналістичних підрозділах для кримінальних розслідувань, а пов'язані з ними системи важко обійти. Розпізнавання відбитків пальців є однією з найбільш зрілих біометричних технологій і підходить для великої кількості програм розпізнавання.

Обличчя. Обличчя є однією з найбільш прийнятних біометричних ознак, оскільки це один із найпоширеніших методів розпізнавання, який люди використовують у повсякденній візуальній взаємодії. Придбання легке і ненав'язливе. Дуже складно розробити алгоритми розпізнавання облич, незмінні до варіацій віку, виразу обличчя, пози та середовища.

Око. Розпізнавання райдужної оболонки – це процес розпізнавання людини шляхом аналізу малюнка райдужної оболонки. Зображення зазвичай отримується за допомогою безконтактного процесу зображення. Розпізнавання не слід плутати з іншою технологією на основі ока, скануванням сітківки. Ефективності розпізнавання райдужної оболонки рідко заважають окуляри або контактні лінзи, і було доведено, що вона надзвичайно точна на зображеннях з високою роздільною здатністю.

Рука. Деякі особливості, пов'язані з рукою людини, є відносно інваріантними та властивими індивіду. Для отримання знімків потрібна

співпраця суб'єкта для зйомки переднього та бічного зображень долоні. За допомогою відповідних приладів (ближнього інфрачервоного випромінювання) можна також розпізнати структуру вени кисті або пальця.

Голос. Отримання голосу не є нав'язливим, і оскільки біометричні ознаки не очікуються в достатній мірі, щоб дозволити ідентифікувати суб'єкт з великої бази даних. Голосовий сигнал залежить від якості пристрою для отримання інформації та залежить від таких факторів, як здоров'я людини, стрес та емоційний стан.

Підпис. Підпис людини називається характеристикою особистості, але вона змінюється з часом і залежить від фізичних та емоційних умов. Підпис протягом тривалого часу прийнятний в державних, юридичних та комерційних операціях як метод перевірки.

1.3 Основи поняття ідентифікації

Ідентифікація особи дає відповідь на запитання: «хто ця особа?» і відноситься до подій, під час яких відбувається перевірка особистості за вказаним переліком унікальних характеристик, що відповідають певній людині.

Процес ідентифікації особистості можна поділити на три етапи:

- визначення та збирання даних - передбачає отримання та колекціонування характеристик ідентифікації, як аргументів для підтвердження особистості;
- перевірка на достовірність зібраних даних - передбачає визначення справжності атрибутів ідентифікації на валідність (непідроблені, підроблені);
- перевірка відношення зібраних даних до певної особистості - передбачає погодження того, що перевірені характеристики пов'язані з конкретно-зазначеною особою.

Деякі характеристики можуть бути однаковими для певної кількості осіб, наприклад вік, ріст чи національність. Тому після колекціонування

характеристик ідентифікації відбувається процес дедублікації, що згруповує відібрані характеристики в один об'єкт ідентифікації, який володіє повною унікальністю, саме через конкретний набір ідентифікаційних характеристик. Потім відбувається відношення між цим унікальним об'єктом ідентифікації та заданою особистістю. Деякі урядові рішення щодо цифрових посвідчень включають процес дедублікації як частину посвідчення особи, що може передбачати перевірку конкретних ознак, таких як біографічні атрибути (наприклад, ім'я, вік та стать), біометрія (наприклад, відбитки пальців, сканування райдужної оболонки або зображення розпізнавання обличчя) та призначені державою атрибути (наприклад, номери паспортів або ідентифікаційний номер платника податків).

Атрибути можуть бути як фізичними (документальними), так і суто цифровими або цифровим представленням фізичних атрибутів (наприклад, цифровий варіант паперових або пластикових водійських прав). Традиційно, посвідчення особи набуло фізичної форми, наприклад, для фізичних осіб виданий державний документ, який включає фотографію володаря документу, голограму або подібні запобіжні заходи. Атрибути також можуть бути невід'ємними - тобто, заснованими на особистих даних особи - біометричні (біологічні або поведінкові) характеристики. Біометрія має швидкий темп розвитку, на сьогоднішній день, породжуючи різні типи біометричних технологій ідентифікації, з різною надійністю та ризиками конфіденційності).

З розвитком цифрових технологій, характеристики ідентифікації тепер можуть створюватися цифровими методами(або конвертуватися з фізичної форми на цифрову) і зберігаються в цифрових базах даних, даючи можливість отримати на відстані ідентифікаційний об'єкт особи та іншу потребувану інформацію про неї, що підлягає дистанційній перевірці та підтвердженню на цифровій основі бази даних.

Аутентифікація відповідає на запитання: «Ви ідентифікований / перевірена особа?». Він визначає, що людина, яка бажає отримати доступ до

облікового запису (або інших послуг чи ресурсів) - це та сама особа, яка пройшла ідентифікацію особи, зареєстрована, а також володіє та контролює обов'язкові атрибути та інші автентифікатори. Надійність автентифікації залежить від типу використовуваних факторів автентифікації та безпеки процесів автентифікації.

Традиційно існує три основні категорії факторів автентифікації. Фактор знання – фактор, який ви знаєте або вам відомий, наприклад: спільний секрет (ім'я користувача, пароль), персональний ідентифікаційний номер (PIN-код) або відповідь на попередньо вибране питання безпеки. Фактори власності - фактор, яким ви володієте, наприклад: криптографічні ключі, що зберігаються в апаратному забезпеченні (у мобільному телефоні, планшеті, комп'ютері чи USB-ключі) або програмному забезпеченні чи; одноразовий пароль, згенерований апаратним пристроєм. Фактор властивості – фактор, який є частиною особистості (біофізична біометрія, така як розпізнавання обличчя та біометрія відбитків пальців або сітківки; біомеханічна біометрія, заснована на унікальному способі взаємодії людини з цифровими пристроями, наприклад, як людина тримає мобільний телефон, гортає екран, або використовує певні комбінації клавіш).

Використання лише факторів автентифікації знань насправді не дає гарної гарантії та не є повністю достовірною адже такі фактори можуть бути відомі іншим особам. Важливо відзначити, що нові види технологічних факторів власності та факторів властивостей (включаючи вдосконалені цифрові автентифікатори пристроїв, біомеханічні біометричні дані та поведінкові біометричні зразки), багато з яких були розроблені або використовуються в основному з метою боротьби з шахрайством.

1.4 Постановка задачі дослідження

Моделі біометричної ідентифікації мають дуже великий потенціал. Однак, алгоритми які використовують біометричні ознаки не є досконалими,

що відображається на їх швидкодії та достовірності кінцевого результату при зміні певних умов. Наприклад, основними проблемами для систем виявлення та розпізнавання обличчя є: умови освітлення, масштаб, поза, фон. Так як весь процес ідентифікації можна розділити на проміжні етапи, то дану проблему можна вирішити шляхом передобробки отриманого зображення, для його покращення та отримання більш чітких рис, і тільки після цього передавати зображення до наступного кроку зчитування. Тому основною задачею даної роботи є детальне дослідження моделей обробки біометричних даних, з метою модифікації їх процесів для покращення часу та точності виконання.

Об'єктом дослідження є моделі ідентифікації за біометричними характеристиками, які є найбільш розповсюдженими для використання (таблиця 1.1).

Таблиця 1.1 – Відношення використання моделей ідентифікації у системах ідентифікації за біометричними характеристиками

Біометричні модель ідентифікації	Відсоток використання у системах біометричної ідентифікації
Обличчя	22,6%
Відбиток пальця	50,1%
Око	16,5%
Інші моделі	10,8%

Для досягнення поставленої мети необхідно вирішити такі задачі:

- проаналізувати сучасні методи розпізнавання обличчя;
- проаналізувати сучасні методи ідентифікації за відбитком пальця;
- проаналізувати сучасні методи ідентифікації за оком;
- визначити можливі методи покращення алгоритмів ідентифікації;
- виконати оптимізацію LBP алгоритму, що використовується для ідентифікації особи за обличчям;

- виконати оптимізацію алгоритму ідентифікації за відбитком пальця, шляхом покращення зображення відбитка;
- виконати покращення алгоритма Хафа, що застосовується на етапі локалізації райдуної оболнки ока.

Досягнення поставленої мети сприятиме використанню моделей біометричної ідентифікації у все більшій кількості проектів де необхідна надійна та швидка система ідентифікації.

2 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ

2.1 Метод Хаар характеристик

Алгоритм біометричної ідентифікації обличчя можна поділити на два основних етапи:

- розпізнавання обличчя на цифровому зображенні;
- порівняння виявленого обличчя з обличчям, що зберігається в системі.

Розпізнавання обличчя - це техніка, яка ідентифікує або відшукує обличчя особи на цифрових зображеннях. Розпізнавання обличчя виконується за допомогою класифікаторів. Класифікатор - це, по суті, алгоритм, який вирішує, чи є дане зображення позитивним (обличчя) чи негативним (не обличчя). Класифікатор потрібно навчати розпізнавати обличчя на тисячах зображень. На щастя, OpenCV уже має два попередньо навчені класифікатори виявлення обличчя, які можна легко використовувати, в даній роботі був використаний Хаар Класифікатор.

Виявлення об'єктів за допомогою каскадних класифікаторів, заснованих на характеристиках Хаара, є ефективним методом виявлення об'єктів. Цей підхід, заснований на машинному навчанні, де функція каскаду тренується з безлічі позитивних і негативних зображень. Потім він використовується для виявлення об'єктів на інших зображеннях.

Спочатку класифікатору потрібно витягти з зображення особливості. Для цього використовується характеристики Хаар, показані на зображенні нижче (рисунок 2.1). Кожна ознака — це одне значення, отримане відніманням суми пікселів під білим прямокутником із суми пікселів під чорним прямокутником.

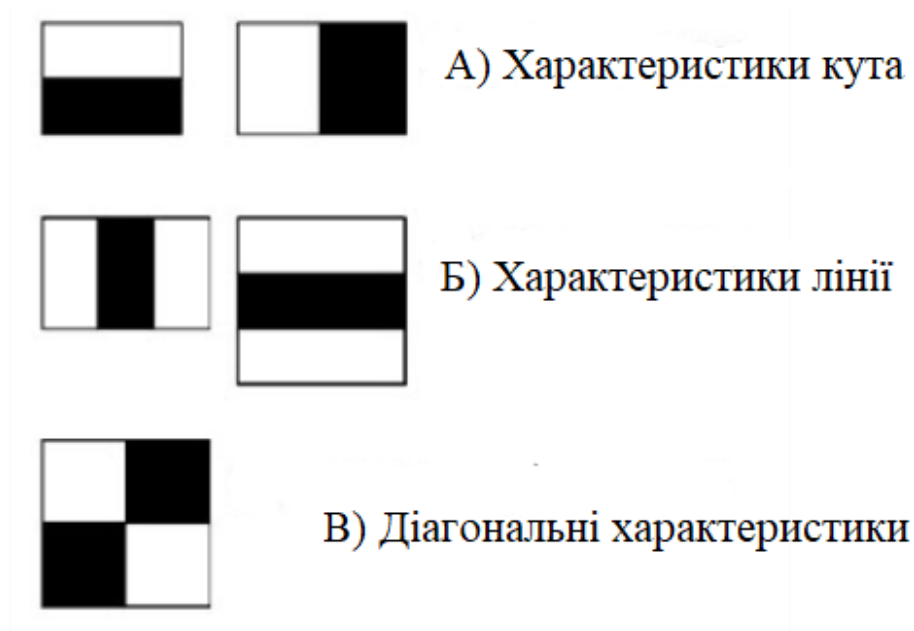


Рисунок 2.1 – Види Хаар характеристик

Для кожного обчислення характеристики нам потрібно знайти суму пікселів під білими та чорними прямокутниками. Для вирішення цієї проблеми потрібно представити зображення в інтегральному виді. Інтегральний вид зображення – це матриця в якій розмірність співпадає з розмірністю зображення. Елементи такої матриці розраховуються за формулою

$$II(x,y) = \text{Summ}(I(i,j)), \quad (2.1)$$

де $I(i,j)$ – яркість пікселя вхідного зображення.

Тобто, кожен елемент (x,y) матриці II складається із суми пікселів вхідного зображення у прямокутнику від координати $(0,0)$ до координати (x, y) . Однією із найефективніших особливостей представлення зображення в інтегральному виді є швидке обчислення суми пікселів довільного прямокутника. Це спрощує обчислення суми пікселів, незважаючи, наскільки великою може бути кількість пікселів.

Але серед усіх цих функцій, які будуть розрахованими, більшість з них

не мають значення. Наприклад, розгляньмо зображення нижче. Верхній рядок показує дві хороші характеристики. Здається, перша обрана характеристика фокусується на властивості того, що область очей часто темніша, ніж область носа та щік. Друга обрана особливість спирається на те, що очі темніші за носову переносицю (рисунок 2.2). Але ті самі особливості, що використовуються на щоках чи будь-якому іншому місці, не мають значення. Щоб відсіяти непотрібні особливості для класифікатора проводять велику кількість тестів на різних зображеннях.



Рисунок 2.2 – Знаходження Хаар особливостей на зображенні

Обличчя може знаходитись на меншій частині зображення. Тож краще застосовувати простий варіант перевірки, чи даний кадр не є обличчям. Якщо ні, то виключаємо його. Натомість зосереджуємось на регіоні, де може бути обличчя. Для відсіювання регіонів зображення де немає обличчя використовують поняття “Каскад класифікаторів”. Всі попередньо відібрані характеристики групуються, до першої групи потрапляє невелика кількість, у кожній наступній групі ця кількість зростає (рисунок 2.3). Якщо регіон зображення не відповідає характеристиці з першої групи, то виключаємо його, регіони, що залишилися перевіряються на наявність характеристик з наступної групи і так далі. Таким чином з усього зображення буде обрана та частина де присутнє обличчя.

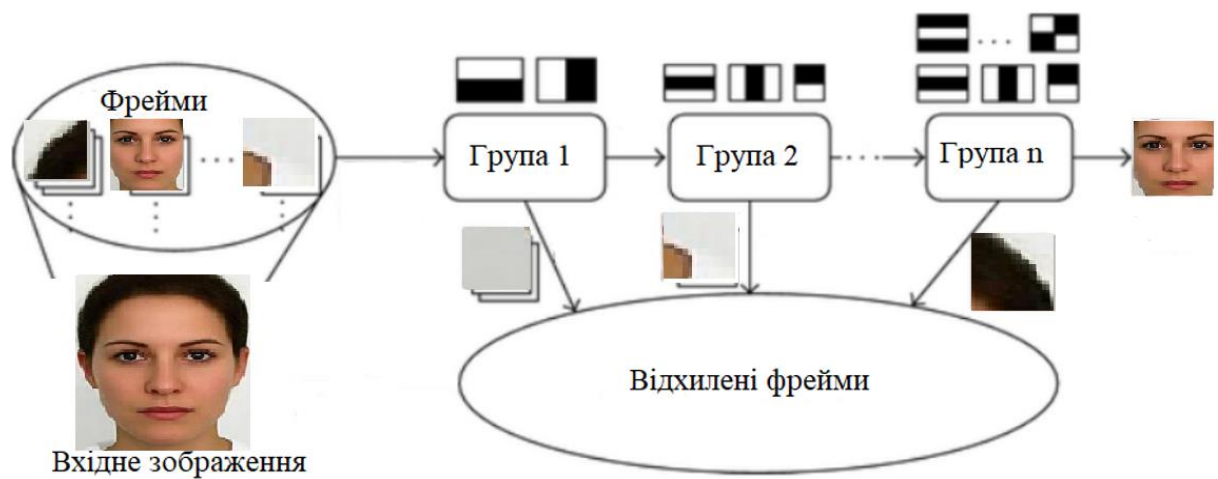


Рисунок 2.3 – Процес пошуку обличчя за особливостями Хаар

Після виявлення обличчя можна переходити до наступного етапу, а саме порівняння з обличчям, що зберігається у системі. Для порівняння обличч існує велика кількість алгоритмів, але для цієї роботи був обраний алгоритм LBPН (Local Binary Patterns Histograms).

Local Binary Pattern Histogram алгоритм – це простий підхід, який позначає пікселі зображення, що обмежують околиці кожного пікселя. Іншими словами, LBPН узагальнює локальну структуру зображення, порівнюючи кожен піксель із сусідами, і результат перетворюється у двійкове число. Вперше він був визначений у 1994 році (LBP), і з того часу виявилось, що це потужний алгоритм класифікації текстур.

Цей алгоритм, як правило, орієнтований на вилучення місцевих особливостей із зображень. Основна ідея полягає не в тому, щоб розглядати ціле зображення як вектор великих розмірів; він фокусується лише на місцевих особливостях об'єкта.

Алгоритм має 4 основних параметри:

- радіус – радіус навколо центрального пікселя, потрібен для побудови локального двійкового шаблону, зазвичай дорівнює 1;
- кількість сусідів – кількість точок для побудови локального двійкового шаблону, зазвичай дорівнює 8 (рисунок 2.4);

- GridX(ширина сітки) – кількість пікселів по осі x для сітки, зазвичай дорівнює 8;

- GridY(довжина сітки) - кількість пікселів по осі y для сітки, зазвичай дорівнює 8.

Відзначаються піксель як центр та його сусіди за параметрами (радіус, кількість сусідів), для побудови локального двійкового шаблону.

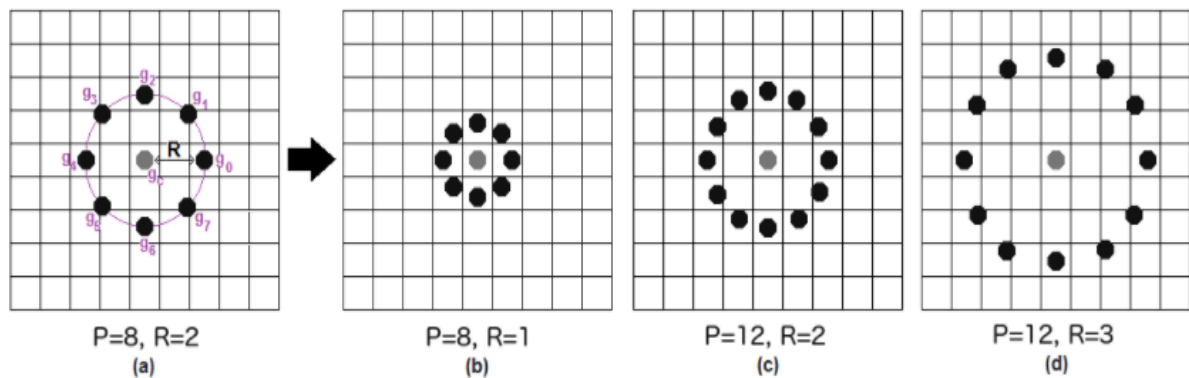


Рисунок 2.4 – Локальний двійковий шаблон при різних параметрах R(радіусу) та P(кількості сусідів)

Якщо інтенсивність центрального пікселя більше-дорівнює його сусіду, тоді позначте його як 1, якщо ні, тоді 0. Маючи 8 сусідніх пікселів, отримаємо $2^8=256$ можливих комбінацій LBP-коду. Таким чином отримаємо двійкове число для кожного пікселя (рисунок 2.5).

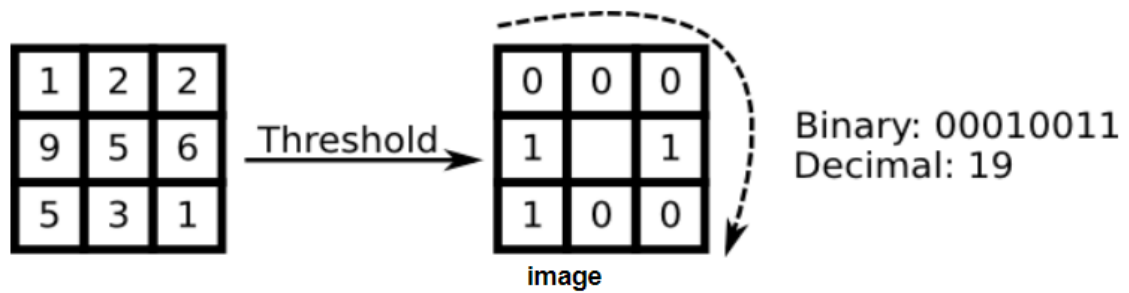


Рисунок 2.5 – Схема визначення LBP-коду

Обчислення LBP використовується для створення проміжного зображення, яке описує вхідне зображення певним чином, виділяючи характеристику обличчя. Цей процес можна розбити на декілька кроків, які детально описані нижче.

припустимо, вхідне зображення обличчя має відтінки сірого;

- отримати частину цього зображення у вигляді вікна розміром 3x3 пікселі;
- можемо використовувати матрицю 3x3, що містить інтенсивність кожного пікселя (0-255);
- потрібно взяти центральне значення матриці, яке буде використовуватися як поріг;
- вибране значення буде використано для визначення нових значень від 8 сусідів;
- для кожного сусіда центрального значення (порога) встановлюється нове двійкове значення, значення 1 встановлюється рівним або вищим за порогове значення, а 0 для значень, нижчим за порогове;
- тепер матриця буде складатися лише з двійкових значень (пропустити центральне значення), потрібно подбати про кожне двійкове значення з кожної позиції з матричного рядка в рядку у нові двійковій матриці (10001101), існують інші підходи до об'єднання двійкових значень (за годинниковою стрілкою), але кінцевий результат буде однаковим;
- двійкове значення перетворюється в десяткове значення і

встановлюються центральне значення матриці, яке становить піксель від вихідного зображення;

- після завершення процедури LBP отримуємо нове зображення, яке представляє кращі характеристики вихідного зображення.

Отримавши зображення з кращими характеристиками, далі можна розбити його на сітку за допомогою параметрів GridX та GridY. Для кожного квадрату сітки будується гістограма. Так як зображення має відтінки сірого, то значення гістограми знаходитимуться у зоні від 0 до 255, що представляє інтенсивність пікселів. Після цього створюється одна глобальна гістограма, шляхом об'єднання всіх попередніх гістограм. Після отримання гістограми вхідного зображення таким же шляхом будуюмо гістограму для зображення, що зберігається в системі, та порівнюємо їх.

2.2 Метод власних обличь (Eigenfaces)

Eigenfaces — це метод виявлення та розпізнавання облич, який визначає дисперсію облич у наборах даних зображень. Він використовує ці відхилення для кодування та декодування облич за допомогою машинного навчання. Набір власних облич — це набір «стандартизованих інгредієнтів облич», визначених статистичним аналізом великої кількості зображень облич. Рисам обличчя присвоюються математичні значення, оскільки цей метод використовує не цифрові зображення, а статистичні бази даних. Будь-яке людське обличчя є комбінацією цих значень з різними відсотками.

Основою методу власних облич є аналіз головних компонентів (РСА). Власні обличчя та РСА були використані Сировичем і Кірбі для ефективного представлення зображень обличчя. Вони почали з групи оригінальних зображення обличчя та розраховували найкращу векторну систему для стиснення зображень. Тоді Турк і Пентланд застосували Eigenfaces для вирішення проблеми з розпізнаванням обличчя.

Аналіз головних компонентів (РСА) — це метод проєкції на підпростір, який широко використовується в шаблонах визнання. Завданням РСА є заміна корельованих векторів великої розмірності на некорельовані вектори меншої розмірності. Іншою метою є обчислення основи для набору даних. Основними перевагами РСА є його низька чутливість до шуму, зниження вимог до пам'яті та ємкості, а також збільшення ефективності за рахунок роботи в просторі менших розмірів.

Стратегія методу Eigenfaces полягає у виділенні характерних рис на обличчі та представлення відповідного обличчя як лінійної комбінації так званих «власних граней», отриманих із об'єкта процесу видобутку.

Розпізнавання досягається за допомогою проєкції грані в простір, утвореної власними гранями. Порівняння на основі евклідової відстані векторів власних граней і власної грані досліджуваного зображення. Якщо ця відстань достатньо невелика, особа ідентифікована. З іншого боку, якщо відстань занадто велика, зображення вважається таким, що належить особі, для якої система має бути навчена.

В якості відправної точки навчальні зображення розмірів $N \times N$ зчитуються і перетворюються на $N^2 \times 1$ розміри. Таким чином створюється навчальний набір розмірів $N^2 \times M$, де M є кількістю зразків зображень. Середнє значення набору зображень розраховується як

$$\psi = \frac{1}{M} \sum_i^M \Gamma \quad (3.1)$$

де ψ середнє зображення, M : кількість зображень, Γ : вектор зображення.

Власні грані, що відповідають найвищим власним значенням, зберігаються. Ці власні грані визначають простір граней. Власний простір створюється проєктуванням зображення на простір граней. Таким чином розмір векторів обчислюються. Розміри зображення налаштовуються відповідно до специфікацій, а зображення покращується етапи попередньої

обробки розпізнавання. Вектор ваги зображення та вектори ваги обличч із бази даних порівнюються.

Обличчя обчислюється та віднімається від кожного обличчя в навчальному наборі. Матриця (A) формується за допомогою результату дії віднімання. Різниця між кожним зображенням і середнім зображенням обчислюється як

$$\phi_i = \Gamma_i - \psi, i = 1, 2, \dots, M \quad (3.2)$$

де ϕ_i це різниця між зображеннями. Матриця, отримана операцією віднімання (A), множиться на її транспонування, отже, коваріаційна матриця C формується:

$$C = A^T A \quad (3.3)$$

Розмірність матриці C дорівнює N x N. M зображень використовуються для формування C. На практиці розміри C дорівнюють N x M. З іншого боку, оскільки ранг A дорівнює M, лише M із N власних векторів є відмінними від нуля. Розраховуються власні значення коваріаційної матриці. Власні грані створюються з використанням кількості навчальних зображень мінус кількість класів (загальна кількість людей) власних векторів.

Вибраний набір власних векторів множиться на матрицю A, щоб створити скорочений підпростір власних граней. Власні вектори менших власних значень відповідають меншим варіаціям коваріаційної матриці. Виразні риси обличчя збережені. Кількість власних векторів залежить від точності, з якою база даних визначена і її можна оптимізувати. Групу вибраних власних векторів називають власними гранями. Коли отримано власні грані, зображення в базі даних проєктуються в простір власних граней і ваги зображення в цьому просторі зберігаються. Для визначення ідентичності зображення порівнюють власні коефіцієнти.

Формується власне обличчя розглянутого зображення. Розраховуються евклідові відстані між власною гранню зображення та власними гранями, збереженими раніше. Особа, про яку йде мова, ідентифікується як така, чия евклідова відстань є мінімальною, нижчою за порогове значення база даних

власних граней. Якщо всі розраховані евклідові відстані більші за порогове значення, то зображення є нерозпізнаним.

Причини вибору методу Eigenfaces для розпізнавання обличчя:

- його незалежність від геометрії обличчя;
- простота реалізації;
- можливість реалізації в реальному часі навіть без спеціального обладнання;
- легкість і швидкість розпізнавання порівняно з іншими методами;
- вищий рівень успіху в порівнянні з іншими методами.

Проблемою методу є час обчислення. Якщо база даних велика, можливо знадобиться деякий час, щоб встановити особу.

2.3 Удосконалення алгоритму ідентифікації обличчя

Можливості алгоритму розпізнавання обличчя LBP сильно залежать від точності виконання етапу виділення та порівняння ознак, що також сильно залежить від якості як вхідних зображень особи, так і навчальних/еталонних зображень, що беруть участь у процесі порівняння осіб. Щоб підвищити точність розпізнавання осіб алгоритмом LBP, було використано наступні властивості якості зображення наших вхідних та еталонних зображень особистості: освітлення, різкість, шум, роздільна здатність, масштаб і поза, щоб отримати зображення найкращої якості, які будуть розкривати більш детальні відомості про функції зображення для більш точного вилучення та порівняння функцій.

Перший крок до покращення полягає у застосуванні методу регулювання контрастності до наших вхідних зображень особи, як визначено у рівнянні

$$g(x, y) = \alpha * f(x, y) + \beta \quad (3.4).$$

Після цього було порівняно три різних фільтри: фільтра розмиття за Гауссом, медіанного фільтра та двостороннього фільтра на точність системи розпізнавання обличчя. Після декількох тестових порівнянь було обрано фільтр, який дає найкращий результат - двосторонній фільтр. Отримані пікселі зображення, вирівнюються за допомогою методу вирівнювання гістограми зображення, щоб остаточно вирішити глобальні проблеми блискавки в оброблених зображеннях обличчя.

Щоб переконатися, що зміни в алгоритмі направлені на поліпшення характеристик виконання ідентифікації алгоритму за обличчям було виконано мовою python реалізацію модифікованого LBP алгоритму (лістинг 2.1), а також алгоритмів Eigenface і LBP, та порівняно їх точність і час виконання. Результати вимірювань надано нижче (таблиця 2.1-2.2).

Лістинг 2.1 – Реалізація мовою Python модифікованого алгоритму розпізнавання обличчя

```
def recognize_face(image):
    result = False
    grayImage=cv2.cvtColor(np.asarray(image),cv2.COLOR_BGR2GRAY)
    faces =
FaceRecognizer.face_cascade.detectMultiScale(grayImage,
scaleFactor=1.5, minNeighbors=5)
    if isinstance(faces, np.ndarray):
        result = True
    return result, faces, grayImage
def authenticate_user(user_id, uploaded_user_face_image,
uploaded_user_face):
    user = User.objects.get(id=user_id)
    client_id = user.clientId.id
    result = False
    if user:
        FaceRecognizer.recognizer.read(
            "face_module/face_recognizer/recognizers/face-
trainer-" + str(client_id) + "-" + str(user.id) + ".yaml")
        for (x, y, w, h) in uploaded_user_face:
            face = uploaded_user_face_image[y:y + h, x:x + w]
            id_, conf = FaceRecognizer.recognizer.predict(face)
            if 4 <= conf <= 85:
                result = True
            else:
```

```

        result = False
    else:
        result = False
    return result, user

```

Таблиця 2.1 – Порівняння точності виконання алгоритмів ідентифікації за обличчям

Назва	Точність виконання %
LBP	85%
Модифікований LBP	93%
Eigenface	89%

Таблиця 2.2 – Порівняння часу виконання алгоритмів ідентифікації за обличчям

Назва	Середній час виконання(мс)
LBP	500
Модифікований LBP	400
Eigenface	500

3 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ВІДБИТКУ ПАЛЬЦЯ

3.1 Загальні положення про ідентифікацію за відбитком пальця

Застосування систем аутентифікації на основі відбитків пальців в останні роки стає дуже популярним не тільки на промисловому або оборонному рівні, але й у пристроях загального призначення, таких як ноутбуки, миші, смартфони, накопичувачі. Слово «відбиток пальця» зазвичай асоціюється з терміном «індивідуальність», але унікальність формально не встановлена, це лише емпіричне спостереження над мільйонами набутих. У цьому розділі ми представляємо опис проблеми розпізнавання відбитків пальців. Починаючи з історичного огляду, ми рухаємося до структурного аналізу відбитків пальців з описом найбільш поширених функцій і баз даних.

Типові застосування біометричної аутентифікації вимагають дуже точного сканування з високою відтворюваністю або комплексної методики аналізу, яка може компенсувати відхилення під час процесу сканування.

Відбитки пальців повністю формуються приблизно на сьомому місяці розвитку плода і залишаються незмінними протягом усього життя людини (властивість стійкості). Якщо виникне поверхневе пошкодження, шкіра відросте в тому ж порядку, що і при народженні. Тому відбитки пальців є надійним засобом ідентифікації на всіх етапах життя людини. Вони навіть є однією з останніх рис, які розкладаються після смерті. Деталі відбитків пальців особи є унікальними для неї і тільки для неї (властивість унікальності). Навіть однайцеві близнюки не мають ідентичних відбитків пальців. Відповідно до припущення про унікальність, різні особи мають різні характерні риси: якщо два відбитки пальців мають багато спільних ознак, то експерт робить висновок, що відбитки пальців належать одній і тій же людині. Припущення про унікальність дозволяє криміналістам запропонувати вагомі докази провини підсудного. Індивідуальність відбитків

пальців все ще детально вивчається.

Отримання відбитка пальця може бути здійснено офлайн або онлайн. При офлайн-зйомці зображення зазвичай отримують шляхом розмазування чорнила на кінчику пальця і створення відбитка чорнилом кінчика пальця на папері. Після цієї процедури відбиток пальця оцифровується оптичним сканером або камерою високої роздільної здатності. Такий відбиток пальця часто називають згорнутим відбитком пальця. Дуже важливим видом офлайнового зображення відбитків пальців є прихований відбиток пальця: часткове зображення відбитка пальця, вилучене з місця злочину судово-медичним експертом. Порівняно зі згорнутим відбитком пальця, прихований відбиток у більшості випадків поганої якості та його важко обробити. При отриманні в Інтернеті відбитку пальця, він отримується за допомогою сканера відбитків без будь-яких видів чорнила. Типовий сканер відбитків пальців містить:

- датчик для зчитування візерунка на поверхні пальця;
- АЦП (аналого-цифровий) перетворювач для перетворення сигналу;
- інтерфейсний модуль, що відповідає за зв'язок із зовнішніми пристроями.

Майже всі існуючі датчики належать до одного з наступних сімейств: оптичні, твердотільні та ультразвукові. Ці датчики ще називають сенсорними (рисунк 4.1). З метою зниження вартості був запропонований інший метод розпізнавання: датчик розгортки, де пальцем проводять по датчику. Це дуже часто зустрічається в мобільних пристроях. Сучасне зчитування відбитків пальців відбувається шляхом прикладання пальця до сенсорної поверхності електронного пристрою зчитування, який сканує та завантажує у відцифрованому вигляді відбиток пальця для додавання до бази даних чи ідентифікації за допомогою додаткового програмного забезпечення. Такі пристрої стали портативними, що дозволяє брати їх із собою та використовувати в різному оточенні та за будь-яких обставин.



Рисунок 3.1 – Пристрій для зчитування відбитку пальця

Проблема сканування відбитка пальця є визначальною для хорошої системи розпізнавання, і існує потреба знайти ефективні методи визначення характерних ознак. Після фази зчитування, за допомогою пристрою, відбитків пальців отримується представлення на основі зображення, що складається з інформації про інтенсивність пікселів, яка не є інваріантною до викривлень, варіацій яскравості, афінних перетворень і вимагає великого обсягу пам'яті. Доступні функції відбитків пальців організовані за рівнями і залежать, зокрема, від роздільної здатності зйомки.

На глобальному рівні відбиток пальця показує згладжену структуру, за винятком однієї або кількох областей, що містять відмінні характеристики, які називаються сингулярностями (рисунок 3.2 та можуть бути:

- дельта (позначається символом Δ);
- цикл (позначений символом $\cap$);
- мутовка (позначається символом O).



Рисунок 3.2 – Відмінні характеристики відбитку пальця

AFIS (Automated Fingerprint Identification System) була представлена на початку 2000-х. Ця система була заснована на методології біометричної ідентифікації, яка використовує технологію цифрових зображень для отримання, зберігання та аналізу даних, пов'язаних з відбитком пальця. Першочергово дану технологію використовували спеціальними службами у США, такими як ФБР, під час розслідувань. Ця технологія використовувала оптичні датчики в якості зчитувачів для сканування та отримання зображення відбитку на послідовних етапах. По-перше алгоритм обробки зображення використовуються для отримання відбитку пальця в відтінках сірого. По-друге, оброблене зображення, таким чином, більше підходить для визначення відмінних характеристик відбитку. І третім етапом є аналіз розміщення відмінних характеристик на відбитку, за допомогою спеціальних алгоритмів. Отримане зображення звіряється зі збереженим в системі, після чого надається результат перевірки. Для знаходження відмінних характеристик використовується спеціальні сітки. На сьогоднішній день розроблено велику кількість сіток для знаходження індивідуальних характеристик відбитку пальця, одним з яких є сітка Осборна. Підхід Осборна полягав у сегментуванні сітки на квадрати однакового розміру, які можуть бути накладені на досліджуванні відбитки таким чином, що квадрат

кожної сітки займає однакове положення на відбитку. Після цього, сітки порівнювалися для підтвердження ідентичності.

3.2 Удосконалення алгоритму ідентифікації за відбитком пальця

Даний розділ зосереджено на вдосконаленні систем розпізнавання відбитків пальців з огляду на три важливі проблеми: покращення відбитків пальців, вилучення основних характеристик відбитків пальців. Поліпшення відбитків пальців і вилучення орієнтації відбитків пальців можна розглядати як кроки попередньої обробки до головної мети в розпізнавання відбитків пальців - автоматичне порівняння з іншими відбитками пальців (відповідність).

Ефективне вилучення помітних ознак відбитків пальців залежить від якості введення відбитка пальця. Якщо якість хороша, потік відбитків пальців добре помітний і надійний набір функцій можна витягти. Якщо відбиток пальця дуже шумний, тоді не можливо виявити з нього надійної інформації: витягується велика кількість помилкових ознак, і пропускається декілька справжніх рис. Тому для досягнення високої продуктивності розпізнавання важливо включити в систему модуль покращення відбитків пальців, здатний покращити якість шумних відбитків пальців, що робить подальші етапи обробки більш надійними. Метою є обчислення одного з найкритичніших параметрів в відбитках пальців, локальна орієнтація: ознака, що позначає напрямок хребетного потоку у дискретних положеннях. Точна оцінка поля локальної орієнтації значно спрощує оцінку інших ознак у відбитків (особливих точок) і покращити продуктивність системи розпізнавання відбитків пальців. Хоча постійно повідомляють про нові розробки та вдосконалення розпізнавання відбитків пальців, часто важко зрозуміти з наукової літератури, які методи є найбільш ефективними і перспективними.

Після короткого огляду найсучасніших технологій розпізнавання відбитків пальців пропонується метод покращення відбитків пальців, який є ітеративним і контекстним. Цей підхід виявляє високоякісні регіони в відбитках пальців, вибірково застосовує контекстну фільтрацію.

Алгоритм вилучення ознак значною мірою залежить від якості введеного відбитка пальця. Якщо якість хороша, течія хребтів-долин добре помітна, і можна отримати надійний набір ознак. Якщо відбиток пальця дуже шумний, алгоритм вилучення дрібниць може виявити велику кількість помилкових ознак і пропустити кілька справжніх ознак. Тому для досягнення високої продуктивності розпізнавання важливо включити модуль покращення відбитків пальців, здатний покращити якість відбитків пальців із шумом, що робить подальші етапи обробки більш надійними.

Алгоритм покращення зображення відбитків пальців отримує вхідне зображення відбитка пальця, застосовує набір проміжних кроків до вхідного зображення і, нарешті, виводить покращене зображення.

Оскільки мета алгоритму покращення відбитків пальців полягає в тому, щоб покращити чіткість структур вхідних зображень відбитків пальців, щоб полегшити наступні етапи обробки, алгоритм покращення відбитків пальців не повинен призводити до створення будь-яких помилкових характеристик. Це дуже важливо, оскільки помилкові виступи або небажані ознаки можуть змінити структуру вхідних відбитків пальців; в результаті індивідуальність може змінитися.

Методи покращення відбитків пальців можна розділити на три групи, які описано нижче.

Методи, що використовують піксельні операції обробки зображень, є найпростішими методами покращення, де інтенсивність пікселя в даній точці залежить від її попереднього значення та глобальних параметрів. Звичайні операції включають нормалізацію, перетворення інтенсивності, обробку гістограми, віднімання зображення, усереднення зображення. Загалом, піксельні методи не дають хороших результатів покращення відбитків

пальців без подальших кроків обробки, зокрема для зображень із шумом. Хороших результатів покращення можна досягти, використовуючи піксельні методи в якості попередньої обробки в передових алгоритмах розпізнавання відбитків пальців.

Методи, що використовують контекстну інформацію, є найпоширенішими підходами до покращення відбитків пальців. Контекст зазвичай представлений локальною орієнтацією, локальною частотою та локальною якістю і використовується для адаптації характеристик фільтра до кожної конкретної області переднього плану.

Для видалення шуму із зображень відбитків пальців за допомогою техніки розкладання та компенсації, яка базується на фільтрі Габора. Фільтри Габора володіють як частотно-селективними, так і орієнтаційно-селективними властивостями і мають оптимальну роздільну здатність як у просторовій, так і в частотній областях. Зображення спочатку розкладається на різні частотні діапазони, а потім на діапазонах низьких і середніх частот очищається хребто-долинний потік і закриваються проміжки, а на високих частотах зберігаються деталі (рисунок 3.3).

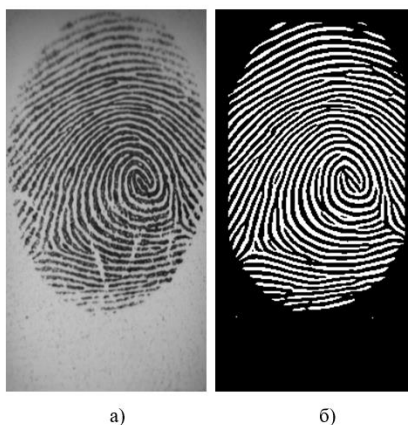


Рисунок 3.3 Результат техніки розкладання та компенсації

Для перевірки позитивного впливу модифікації алгоритму, було виконано мовою python його реалізацію (лістинг 3.1) і порівняно час та точність виконання із звичайною реалізацією (таблиці 3.1-3.2).

Лістинг 3.1 – Фрагмент реалізації мовою Python етапу нормалізації модифікованого алгоритму ідентифікації за відбитком пальця

```

from .ridge_segment import ridge_segment
from .ridge_orient import ridge_orient
from .ridge_freq import ridge_freq
def image_enhance(img):
    blksize = 16; thresh = 0.1;
    normim,mask = ridge_segment(img,blksize,thresh);
    gradientsigma = 1; blocksigma = 7; orientsmoothsigma= 7;
    orientim      =      ridge_orient(normim,      gradientsigma,
blksize, windsigma, orientsmoothsigma);
    blksize = 38; windsigma = 5; minWaveLength = 5;
    maxWaveLength = 15;
    freq,medfreq  =  ridge_freq(normim,  mask,  orientim,
blksize, windsigma, minWaveLength,maxWaveLength);
    freq = medfreq*mask; kx = 0.65; ky = 0.65;
    newim = ridge_filter(normim, orientim, freq, kx, ky);

```

Таблиця 3.1 – Порівняння точності виконання звичайного алгоритму з модифікованим

Назва	Точність виконання %
Звичайний алгоритм	85%
Модифікований	91%

Таблиця 3.2 – Порівняння часу виконання звичайних алгоритмів з модифікованим

Назва	Середній час виконання(мс)
Звичайний алгоритм	450
Модифікований	400

4 МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОКА

4.1 Загальні положення про ідентифікацію ока

Розпізнавання райдужної оболонки ока та сканування сітківки ока — це технології біометричної ідентифікації на основі ока, які використовуються як рішення для запобігання шахрайству. Це означає, що вони покладаються на унікальні фізіологічні характеристики ока, щоб ідентифікувати людину. Незважаючи на те, що за своєю суттю може здатися, що процес схожий або навіть однаковий, насправді вони досить різні.

Сітківка ока - тонка тканина нервових клітин, що вистилає задню стінку ока. Сітківка містить кілька шарів сенсорної тканини та мільйони фоторецепторів. Цей шар тканини виявляє світло та створює електричні імпульси, які надсилаються через зоровий нерв до мозку, що дозволяє людині бачити. Іншими словами, сітківка в основному діє як датчик зображення в камері. Нейрональна сітківка, що складається з кількох шарів нейронів, примикає до серії синапсів, де зовнішній шар пігментованих епітеліальних клітин підтримує її. Основні світлочутливі клітини сітківки ока складаються з двох специфічних типів фоторецепторних клітин: паличок і колбочок. У той час як палички зазвичай функціонують в умовах слабкого освітлення та відповідають за чорно-білий зір, колбочки створені для більш яскравого освітлення та відповідають за розпізнавання кольорів. Рівень унікальності настільки високий, що навіть однойцеві близнюки не мають однакового малюнка капілярів. Протягом усього життя людини структура сітківки зазвичай залишається незмінною, хоча трапляються виключення, коли людина хворіє певними захворюваннями, такими як глаукома, діабет або дегенеративні захворювання сітківки.

Під час сканування сітківки ока зчитується унікальний малюнок сітківки ока людини. Кровоносні судини сітківки можна ідентифікувати за

допомогою спеціального освітлення. Сканування сітківки виконується шляхом потрапляння променя інфрачервоного світла низької енергії в око людини, яка дивиться в окуляр сканера з близької відстані. Кількість відбитого світла змінюється, коли світло проходить через сітківку. Далі відбувається відхилення у відображенні, яке спричинене тим, що кровоносні судини сітківки поглинають більше світла від світлового променя, ніж решта ока. Потім в базу даних зберігається отриманий код, який утворюється з шаблону варіацій. Сканування сітківки є однією з найточніших форм біометричної технології з рівнем похибки 0,0001%. Це робить його потужним рішенням для запобігання шахрайству для команд безпеки.

Райдужка — це тонка кругла структура в передній частині людського ока. Вона відповідає за розмір і діаметр зіниць, що визначає, скільки світла досягає сітківки. Райдужна оболонка визначає колір очей, і він відрізняється від людини до людини. Чим більше стає зіниця, тим більше світла проникає в сітківку.

Історія розпізнавання райдужної оболонки відносно молода. Все почалося в 1936 році, коли офтальмолог Френк Берч виявив відмінності між людськими райдужними оболонками і запропонував візерунки як метод розпізнавання людей. Однак лише в 1987 році лікарі Леонард Флам і Аран Сафір отримали патент на концепцію ідентифікації райдужної оболонки ока, засновану на ідеї, що немає двох однакових райдужних оболонок. Зростання розпізнавання райдужної оболонки ока як методу ідентифікації відбулося відразу після закінчення терміну дії патентів і технологія була готова до широкої комерціалізації.

Оскільки малюнок райдужної оболонки залишається практично незмінним протягом усього життя людини, розпізнавання райдужної оболонки є одним із найточніших біометричних методів, які зазвичай застосовуються. Рівень хибного прийняття та хибного відхилення при скануванні райдужної оболонки надзвичайно низький, що гарантує вищий рівень точності перевірки особи та автентифікації.

Під час сканування райдужної оболонки використовується технологія камери для отримання зображень райдужної оболонки за допомогою інфрачервоного світла. Сканування райдужної оболонки ока дає детальне зображення, що відображає складну структуру райдужної оболонки. Потім зображення можна перетворити на математичний і статистичний шаблон, який може ідентифікувати особу. Бази даних містять ці шаблони та знаходяться відповідними механізмами з надзвичайно високою швидкістю. Частота помилкових збігів із цією технологією нескінченно мала. Технологія точна приблизно на 90-99%. Це робить його масштабованим рішенням для різних компаній, орієнтованих на безпеку.

Розпізнавання райдужної оболонки ока є простою у використанні технологією, при якій людині потрібно лише стояти нерухомо перед камерою, а про все інше подбає технологія, що стоїть за нею. Не потрібен прямий фізичний контакт між людиною та камерою, що робить розпізнавання райдужної оболонки абсолютно ненав'язливим.

Будучи однією з нових біометричних технологій, розпізнавання райдужної оболонки має відносно високу вартість. Сканери райдужної оболонки досить дорогі, що робить їх доступними для урядів і великих корпорацій. Щоб розпочати надійний процес розпізнавання райдужної оболонки, необхідне належне налаштування. Може знадобитися більше ніж кілька спроб, щоб отримати правильний процес захоплення, оскільки сканери очей можуть бути чутливими до відбиття. Крім того, вони вимагають від людини нерухомості та уникнення зайвих рухів. Незважаючи на складності під час роботи з обладнанням, швидкість сканування райдужної оболонки та видимість ока, а також неймовірно низький рівень помилкових збігів є одними з головних причин, чому ця біометрична технологія набуває популярності.

Розпізнавання райдужної оболонки ока можна використовувати в різноманітних програмах, таких як безпека в аеропортах, конфіденційні будівельні завдання та військові операції. Розпізнавання райдужної оболонки

ока також може забезпечити унікальну особу для громадян, які не мають паспорта чи іншого посвідчення особи, надаючи їм доступ до державних послуг.

Основна схожість між скануванням райдужної оболонки та скануванням сітківки ока полягає в тому, що вони обидва використовують людське око для ідентифікації. Деякі інші подібності між двома біометричними методами включають:

- низький рівень помилкових спрацьовувань;
- помилково негативні показники низькі;
- надійний біометричний метод, оскільки жодна людина не має однакового малюнка райдужки або сітківки;
- обидва методи швидко автентифікують індивідуальні особи;
- ампутоване око не можна використовувати для отримання доступу, оскільки і райдужка, і сітківка надто швидко розкладаються;

Хоча як сканування райдужної оболонки, так і сканування сітківки ока використовують очі для біометричної ідентифікації людини, вони помітно відрізняються один від одного. З одного боку, сканування райдужної оболонки використовує технологію камери для отримання зображення райдужної оболонки. Це робить його придатним для використання у сценаріях відсутності клієнта, що стає все більш поширеним явищем у епоху цифрових технологій. Сканування райдужної оболонки вважається неінтрузивним методом біометричної ідентифікації, оскільки зображення райдужної оболонки можна отримати на відстані.

Сканування сітківки, з іншого боку, вимагає сканування пучка світла глибоко всередині ока, щоб отримати зображення сітківки. Для цього потрібне спеціальне обладнання що краще підходить для процедур ідентифікації особи. Сканування сітківки — це метод біометричної ідентифікації, який більш інвазивний, ніж сканування райдужної оболонки, оскільки сітківка розташована на задній частині ока. З цієї причини воно менш прийнятне, ніж сканування райдужної оболонки ока.

Деякі інші відмінності між двома рішеннями для запобігання шахрайству включають:

- сітківка ока може бути змінена через захворювання, тоді як райдужка залишається переважно стабільною;
- сканування райдужної оболонки ока фіксує зображення райдужної оболонки ока на відстані, тоді як сканування сітківки ока робить це шляхом розміщення ока людини поблизу окуляра;
- сканування сітківки найкраще підходить для фізичної ідентифікації;
- сканування райдужної оболонки може відбуватися у фізичному та цифровому сценаріях;
- сканування сітківки займає більше часу, ніж сканування райдужки;
- сканування райдужної оболонки ока є більш прийнятним для комерційного використання, ніж сканування сітківки ока;

4.2 Ідентифікація особистості за райдужною оболонкою

Так само як і інші способи ідентифікації особи, цей можна розділити на основні етапи (рисунок 4.1). На кожному етапі, окрім зчитування райдужної оболонки, цей етап було замінено на готові знімки ока, використовуються певні алгоритми які було досліджено в даній роботі.

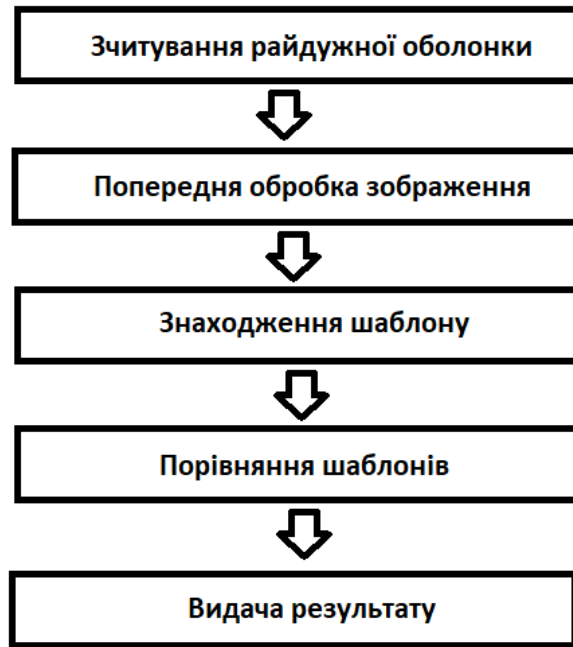


Рисунок 4.1 – Основні етапи розпізнавання особистості за райдужною оболонкою ока

4.2 Моделі локалізації райдужної оболонки

Попередня обробка зображення райдужної оболонки розділена на три кроки (рисунок 4.2): локалізація райдужної оболонки, нормалізація райдужної оболонки та покращення зображення.

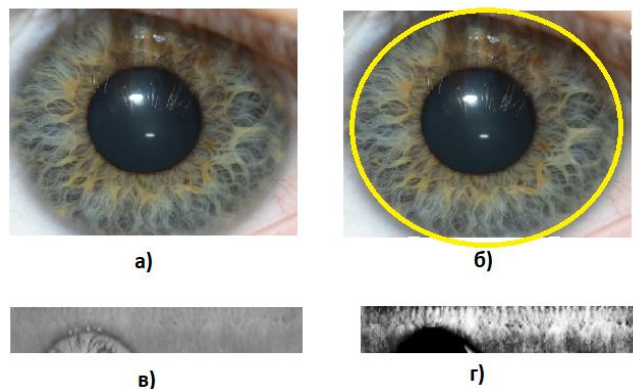


Рисунок 4.2 – Кроки попередньої обробки зображення: а) нормальне зображення б) локалізація; в) нормалізація; г) покращення

Локалізація райдужної оболонки за методом Хафа визначає межі райдужної оболонки. межі райдужної оболонки можна приблизно змодельовати як кола. Локалізація райдужної оболонки важлива, оскільки правильна область райдужної оболонки необхідна для створення шаблонів точного підбору. Серед методів локалізації відомі такі як, інтегро-диференціальний оператор, перетворення Хафа, дискретний круговий активний контур, метод розрізу навпіл і метод пошуку чорної діри.

Інтегро-диференціальний оператор використовується для визначення зовнішньої межі райдужної оболонки, а також верхньої та нижньої повік (рисунок 4.2 (б)). Оператор обчислює часткову похідну середньої інтенсивності точок кола по відношенню до збільшення радіуса r . Після згортки оператора з ядром Гауса максимальна різниця між внутрішнім і зовнішнім колом визначатиме центр і радіус межі діафрагми. Для виявлення верхньої та нижньої повік шлях контурної інтеграції змінено з кругової на параболічну криву. Оператор є точним, оскільки він шукає в області зображення глобальний максимум. Він може обчислювати швидше, оскільки використовує першу похідну інформацію.

Оскільки внутрішню межу райдужної оболонки можна моделювати як коло, для локалізації райдужної оболонки використовується кругове перетворення Хафа. По-перше, детектор країв застосовується до зображення райдужної оболонки в градаціях сірого для створення карти країв. Карту краю отримують шляхом обчислення першої похідної від значень інтенсивності та порогового значення результатів. Фільтр Гауса застосовано для згладжування зображення для вибору належного масштабу аналізу країв. Процедура голосування реалізована за допомогою перетворення Хафа для пошуку потрібного контуру на карті країв. Припускаючи коло з координатою центру (x_c, y_c) і радіусом r , кожна реберна точка кола дає право голосу. Центральна координата та радіус кола з максимальною кількістю голосів визначається як основний контур. Для виявлення повік, контур визначається за допомогою параметра параболічної кривої замість параметра кола. Для

створення карти країв потрібне порогове значення. Вибране порогове значення може видалити критичні крайові точки та призвести до помилкового виявлення кола.

Для локалізації райдужної оболонки також використовували активну контурну модель. Контур визначається як набір з n вершин, з'єднаних як проста замкнена крива. Рух контуру викликається внутрішніми і зовнішніми силами, що діють на вершини. Внутрішні сили розширюють контур до ідеального кола. Зовнішні сили штовхають контур усередину. Контур рухається під впливом внутрішніх і зовнішніх сил, доки не досягне рівноваги. Середній радіус і центр отриманого контуру є параметрами межі райдужної оболонки. Це впливає на пошук дискретного кругового активного контуру для їх межі завдяки дзеркальному відображенню від рогівки. Тому для видалення дзеркальних відображень необхідний алгоритм попередньої обробки зображення.

Визначення країв застосовується до зображення райдужної оболонки, щоб отримати інформацію про краї. Для кожних двох точок на тому самому компоненті краю застосовується метод розділення навпіл, щоб провести перпендикулярні лінії до центральної точки. Центральна точка з максимальною кількістю перетинів ліній вибирається як центр зіниці. Віртуальне коло малюється відносно центру зіниці, а радіус збільшується в певному діапазоні. Віртуальне коло з найбільшою кількістю крайових точок вибрано як межу райдужної оболонки. На метод розрізу навпіл впливає нерівномірне освітлення та відбиття. Як наслідок, їх внутрішню межу неможливо локалізувати точно. Подібно до методу дискретного кругового активного контуру, алгоритм попередньої обробки зображення необхідний для видалення областей високої інтенсивності, викликаних освітленням і відображенням.

Метод пошуку чорної діри використовується для обчислення центру та площі зіниці. Оскільки зіниця є найтемнішою областю на зображенні, цей підхід застосовує метод сегментації порогів, щоб знайти область. По-перше,

визначається поріг для визначення темних областей на зображенні райдужної оболонки. Темні області називаються «чорними дірами». Центр маси цих чорних дір обчислюється на основі глобального зображення. Площа зіниці – це загальна кількість цих чорних дір у регіоні. Радіус зіниці можна обчислити за формулою площі кола. Метод пошуку чорної діри не підходить для зображення райдужної оболонки з темною райдужною оболонкою. Замість області зіниці буде виявлено темну область райдужки.

4.3 Алгоритми знаходження шаблону райдужної оболонки

На етапі знаходження шаблону використовуються методи аналізу текстури, щоб виділити відмінні характеристики з попередньо-обробленого зображення райдужної оболонки. Отриманні дані будуть закодовані для створення біометричного шаблону.

Кожен шаблон демодулюється для вилучення його фазової інформації за допомогою квадратурних двовимірних вейвлетів Габора. Інформація про фазу квантується в чотири квадранти в комплексній площині. Кожен квадрант представлений двома бітами інформації про фазу. Таким чином, кожен піксель у нормалізованому зображенні демодулюється в двобітовий код у шаблоні. Інформація про фазу витягується, оскільки вона надає важливу інформацію всередині зображення. Однією з переваг даного підходу є те, що він не залежить від сторонніх факторів, таких як контраст зображення, освітленість і посилення камери. Він являє собою смуговий фільтр для видалення компонентів, викликаних фоновою яскравістю.

Вейвлет-перетворення розкладає область райдужної оболонки на компоненти з різною роздільною здатністю. Зазвичай використовуються вейвлети Добеші, Біртогональні та мексиканського капелюха. Перевага вейвлет-перетворення над перетворенням Фур'є полягає в тому, що воно має просторову роздільну здатність і роздільну здатність по частоті. Функції локалізовані як у просторовій, так і в частотній областях із змінними

розмірами вікон. Вейвлет-фільтрів застосовується до нормалізованої області райдужної оболонки. Кожен фільтр налаштовано на кожну роздільну здатність із кожним вейвлетом, визначеним функціями масштабування. Вихідні дані фільтрів кодуються для створення компактного біометричного шаблону.

Фільтри Лапласа Гауса використовуються для кодування ознак шляхом розкладання області райдужної оболонки. Відфільтроване зображення реалізовано як піраміда Лапласа. До зображення застосовано каскад фільтрів, подібних до Гауса. Піраміда Лапласа складається з чотирьох рівнів для створення компактного біометричного шаблону. Цей підхід стискає дані для отримання значущих даних. Стислі дані можна зберігати та ефективно обробляти.

На відміну від інших біометричних даних, таких як відбитки пальців і обличчя, чіткий аспект райдужної оболонки ока походить від випадково розподілених рис. Це призводить до його високої надійності для ідентифікації особистості та, водночас, до труднощів у ефективному представленні таких деталей на зображенні. Для представлення характеристик райдужної оболонки використовуються ключові локальні варіації. Основна ідея полягає в тому, що локальні різкі точки варіації, що позначають появу або зникнення важливої структури зображення, використовуються для представлення характеристик райдужної оболонки. Вся процедура виділення ознак включає два етапи:

- створюється набір одновимірних сигналів інтенсивності для ефективної характеристики найважливішої інформації вихідного двовимірного зображення;
- використовуючи певний клас вейвлетів, послідовність позицій локальних гострих точок варіації в таких сигналах записується як особливості.

Нормалізоване зображення райдужної оболонки розкладається на набір одновимірних сигналів інтенсивності. До кожного сигналу застосовується

вейвлет-перетворення. Локальні екстремуми результатів вейвлет-перетворення відповідають різким коливанням інтенсивності вихідного сигналу. Локальні точки максимуму та мінімуму кодуються у вектор ознак. Вектор ознак перетворюється на бінарний шаблон такого ж розміру, що й нормалізоване зображення райдужної оболонки.

Райдужна оболонка кодується на основі різниці коефіцієнтів дискретного косинусного перетворення (DCT) прямокутних ділянок. Нормалізоване зображення розділене на діагональні ділянки 8x12. Середнє значення за шириною визначається вікном із використанням вікна Ханнінга для зменшення впливу шуму. Подібне вікно Ханнінга та DCT застосовано до ділянки вздовж його довжини. Отримують різниці між коефіцієнтами DCT сусідніх ділянок. Абінарний шаблон генерується з перетинів нуля різниць між коефіцієнтами DCT. Цей метод кодування має низьку складність і гарне розділення між класами. Він перевершує інші підходи як за швидкістю, так і за точністю.

Перетворення Гільберта використовується для отримання важливої інформації з текстури райдужної оболонки. Аналітичне зображення будується за вихідним зображенням і його перетворенням Гільберта. Його можна використовувати для аналізу текстури райдужної оболонки. Частота появи та миттєва фаза обчислюються з аналітичного зображення. Виникаюча частота формується трьома різними домінуючими частотами аналітичного образу. Миттєва фаза - це арктангенсна функція дійсної та уявної частин аналітичного зображення. Вектор ознаки кодується шляхом визначення порогової частоти виникнення та миттєвої фази. Перевагою цього підходу є обчислювальна ефективність. Фільтрація виконується в домені Фур'є за допомогою чистих реальних фільтрів.

4.4 Методи порівняння шаблонів райдужної оболонки

Шаблони, створені на етапі вилучення функцій, потребують

відповідної метрики. Метрика відповідності порівнює подібність між шаблонами. Порогове значення встановлюється для розрізнення внутрішньокласових і міжкласових порівнянь.

Відстань Хеммінга визначається як дробова міра відмінності між двома бінарними шаблонами. Значення нуль представлятиме ідеальний збіг. Два повністю незалежні шаблони дадуть відстань Хеммінга близько 0,5. Порогове значення встановлюється, щоб визначити, що два шаблони належать одній особі чи різним особам. Дробова відстань Хеммінга є сумою виключного або між двома шаблонами на загальну кількість бітів. Шаблони маскування використовуються в розрахунку для виключення областей шуму. Під час обчислення використовуватимуться лише ті біти в шаблонах, які відповідають «1» біту в шаблоні маскування. Перевагою відстані Хеммінга є швидке узгодження, оскільки шаблони мають двійковий формат. Час виконання для порівняння вимикаючого або двох шаблонів становить приблизно 10 мкс. Відстань Хеммінга підходить для порівняння мільйонів шаблонів у великій базі даних.

Зважена евклідова відстань використовується для порівняння двох шаблонів для ідентифікації райдужки. Шаблони складаються з цілих значень. Зважена евклідова відстань визначається як міра подібності між двома шаблонами. Він обчислюється за допомогою теореми Піфагора, щоб отримати відстань між двома точками. Шаблон райдужної оболонки порівнюється з усіма шаблонами в базі даних. Два шаблони збігаються, якщо зважена евклідова відстань є мінімальною.

Нормована кореляція між двома представленнями розраховується для відповідності. Він визначається як нормалізована подібність відповідних точок в області райдужки. Кореляції виконуються над невеликими блоками пікселів у чотирьох різних діапазонах просторових частот. Нормалізована кореляція враховує локальні варіації інтенсивності зображення. Однак нормалізований метод кореляції не є ефективним з точки зору обчислень, оскільки для порівняння використовуються зображення.

Найближча ознакова лінія є ефективним методом класифікації на етапі узгодження шаблонів. Характерна лінія проходить через будь-які дві характерні точки одного класу. Характерна лінія виділяє більше варіацій вектора ознак, ніж характерні точки. Розраховується відстань від характерної точки до характерної лінії. На етапі класифікації буде використано найближчу відстань до характерної лінії

4.5 Удосконалення алгоритму ідентифікації за оком

Як уже було зазначено вище, алгоритм ідентифікації особи складається з декількох основних етапів, які в свою чергу також можуть виконуватися послідовно в певну кількість кроків. Тому зміни для покращення роботи алгоритму були направлені саме на ці етапи.

Обидві межі (внутрішня межа і зовнішня межа) типової райдужної оболонки можна приблизно прийняти як кола. Спочатку орієнтовно визначається область райдужки у вихідному зображенні, а потім використовується виявленням країв, щоб точно обчислити параметри двох кіл у визначеному регіоні.

Проектується зображення у вертикальному та горизонтальному напрямках, щоб приблизно визначити координати центру зіниці ока (x_3, y_3) . Так як зіниця, як правило, темніше ніж райдужка, відповідні координати розглядаються як мінімуми двох проекційних профілів координат центру зіниці

$$x_p = \arg \min(\sum I(x,y)), y_p = \arg \min(\sum I(x,y)) \quad (4.1)$$

де x_p та y_p позначають координати центру зіниці в оригінальному зображенні.

Обчислюється більш точна оцінка координат центру зіниці. Область з розмірами 120 x 120 з центром у точці (x_3, y_3) бінаризується, адаптивно вибираючи прийнятне порогове значення за допомогою гістограми рівня сірого цієї області. Центроїд отриманої бінарної області розглядається як

нова оцінка координат зіниці. Можна підвищити точність оцінки центру координати зіниці, повторюючи цей крок, починаючи з координати, оціненої за допомогою проекції зображення. Після цього обчислюються точні параметри цих двох кіл за допомогою виявлення краю та перетворення Хафа в певній області, що визначається центром зіниці.

У порівнянні зі звичайним методом локалізації Хафа де також використовується комбінація визначення краю та перетворення, представлений метод наближає область райдужної оболонки до виявлення краю та перетворення Хафа. Це зменшить область для виявлення країв і простір пошуку перетворення Хафа, що призведе до зниження обчислювальних витрат.

Райдужки різних людей можуть бути різного розміру, і навіть для райдужок одного ока розмір може змінюватися через варіації освітлення та зміни відстані між камерою та оком. Така форма деформації текстури райдужної оболонки вплине на результати порівняння. Для отримання більш точних результатів розпізнавання необхідно компенсувати таку деформацію. Для можна представити райдужку за допомогою фіксованого інтервалу параметрів у подвійно безрозмірній псевдополярній системі координат, тоді. Далі відбувається розгортання кільцеподібної райдужної оболонки проти годинникової стрілки до прямокутного блоку текстури фіксованого розміру. Нормалізація не тільки зменшує до певної міри викривлення райдужної оболонки, спричинене рухом зіниці, але й спрощує подальшу обробку.

Нормалізоване зображення райдужної оболонки (рисунок 4.3) має низький контраст і може мати нерівномірну яскравість через розташування джерел світла. Усе це може вплинути на подальшу обробку під час вилучення ознак і зіставлення. Щоб отримати більш добре розподілене текстурне зображення, запускається процес апроксимацій варіації інтенсивності по всьому зображенню. Середнє значення кожного маленького блоку, розмірами 16 x 16 становить приблизну оцінку фонового освітлення. Ця оцінка додатково розширюється до того самого розміру, що й

нормалізоване зображення, шляхом бікубічної інтерполяції. Розрахункове фонове освітлення, віднімається від нормалізованого зображення, щоб компенсувати різні умови освітлення.



Рисунок 4.3 – Нормалізоване зображення райдужки ока

Потім зображення з корекцією освітлення покращується за допомогою вирівнювання гістограми в кожній області, яка має розміри 32 x 32. Така обробка компенсує нерівномірність освітлення, а також покращує контрастність зображення (рисунок 4.4).



Рисунок 4.4 – Покращене зображення райдужки ока

Як згадувалося раніше, характеристики райдужної оболонки можна розглядати як свого роду перехідні сигнали. Локальні різкі варіації зазвичай використовуються для характеристики важливих структур перехідних сигналів. Таким чином, ми створюємо набір одновимірних сигналів інтенсивності, які здатні зберігати найрізкіші варіації оригінального зображення райдужної оболонки. Вейвлет-перетворення є особливо популярним підходом до аналізу сигналів і широко використовується в обробці зображень. У цій статті використовується спеціальний клас одновимірних для представлення результуючих одновимірних сигналів інтенсивності. Положення локальних гострих точок варіації записується як особливості.

Локальні деталі райдужної оболонки зазвичай розповсюджуються

вздовж радіального напрямку на вихідному зображенні, що відповідає вертикальному напрямку на нормалізованому зображенні. Таким чином, щільність інформації в кутовому напрямку, що відповідає горизонтальному напрямку в нормалізованому зображенні, набагато вища, ніж в інших напрямках; тобто може бути достатньо лише зафіксувати локальні різкі коливання вздовж горизонтального напрямку нормалізованого зображення, щоб охарактеризувати райдужку. Крім того, оскільки основна ідея полягає в тому, щоб представити випадково розподілені блоки райдужної оболонки за допомогою характеристики локальних різких варіацій райдужної оболонки, немає необхідності фіксувати локальні різкі точки варіації в кожному рядку зображення райдужної оболонки для розпізнавання. Маючи на увазі ці два аспекти, 2-D нормалізоване зображення розкладається на набір 1-D сигналів інтенсивності. По суті, кожен сигнал інтенсивності є комбінацією послідовних горизонтальних ліній сканування, які відображають локальні зміни об'єкта вздовж горизонтального напрямку. Набір таких сигналів містить більшість локальних різких варіацій райдужної оболонки. Крім того, така обробка зменшує обчислювальні витрати, необхідні для подальшого представлення ознак.

Нижче представлено порівняння звичайних алгоритмів з модифікованим (таблиці 4.1-4.2), який було реалізовано за допомогою мови Python (лістинг 4.1)

Лістинг 4.1 – Фрагмент реалізації мовою Python модифікованого етапу локалізації за методом Хафа

```
imgs = []; label=0; final_output = []; lables = []
for filepath in glob.iglob('test/*'):
    if filepath[-1] == 'g':
        img = cv2.imread(filepath);img=cv2.resize(img, (200,150))
        img=cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        imgs.append([img,filepath])
for filepath in glob.iglob('UBIRIS_200_150/Sessao_1/*'):
    num_in_folder= 0
```

```

iris_num=0
for i,j,L,c in imgs:
    circles = cv2.HoughCircles(i, cv2.HOUGH_GRADIENT, 10, 100)
    if circles is not None :
        circles = np.round(circles[0, :]).astype("int")
        maxiumum_average=100000000000000; key=True
        for (x, y, r) in circles:
            if x+r<=max(i.shape) and y+r<=max(i.shape) and x-r>0
and y-r>0 and r>20:
                key=False; new_roi = i[y-r:y+r, x-r:x+r]
                average = np.average(new_roi)
                if average < maxiumum_average:
                    maxiumum_r = r; point_x=x
                    point_y=y; maxiumum_average=average
        if key:
            print("key opened")
            for (x, y, r) in circles:
                maxiumu_raduis=-4
                if r > maxiumu_raduis:
                    maxiumum_r = r; point_x=x
                    point_y=y
                    maxiumum_average=average
            cv2.circle(c, (point_x, point_y), maxiumum_r, (255, 255,
0), 4)

```

Таблиця 4.1 – Порівняння точності виконання звичайних алгоритмів з модифікованим

Назва	Точність виконання %
Метод Хафа	89%
Метод контурної моделі	90%
Модифікований метод Хафа	89%

Таблиця 4.2 – Порівняння часу виконання звичайних алгоритмів з модифікованим

Назва	Середній час виконання(мс)
Метод Хафа	700
Метод контурної моделі	650
Модифікований метод Хафа	500

5 ВИБІР ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РЕАЛІЗАЦІЇ

5.1 Огляд технологій

У кваліфікаційній роботі було використано такі технології як операційна система Windows, мова програмування Python, фреймворк django та бібліотека OpenCV. Так як основною метою данної роботи є саме порівняння алгоритмів ідентифікації з їх подальшим покращенням, то використання бази даних не є раціональним, всі зображення збережено в файловій системі віндовс. Як IDE було використано PyCharm. Розглянемо ці технології докладніше.

5.2 Мова програмування Python

Мова програмування Python була обрана як потужний мультизадачний інструмент для розробки програмного забезпечення. Python був використаний для реалізації алгоритмів ідентифікації за різними біометричними ознаками. Синтаксис Python було імплементовано таким чином, щоб була можливість його прочитати та зрозуміти навіть тим, хто тільки починає його вивчати. Неймовірна простота перетворює Python на ідеальний інструмент для програмування, з можливістю швидко в ньому розібратися. Як результат, розробники витрачають більше часу на обдумування проблеми, яку намагаються вирішити, і менше часу на роздуми про мовні складності чи розшифровку коду, залишеного іншими.

Python є популярним і широко використовуваним, займає високі рейтинги в опитуваннях і має велику кількість проектів GitHub, які використовують цю мову. Python є кросплатформенною мовою програмування та підтримує основні операційні системи і платформи, а також деякі другорядні. Багато основних бібліотек і служб на основі API

мають прив'язки або обгортки Python, які дозволяють вільно взаємодіяти з цими службами або безпосередньо використовувати бібліотеки. Кожна нова версія мови Python додає нові корисні функції, щоб не відставати від сучасної практики розробки програмного забезпечення. Наприклад, асинхронні операції тепер є стандартною частиною мови, що полегшує написання програм Python, які виконують одночасну обробку. Важливим аспектом Python є його динамічна природа. Усе в мові, включаючи самі функції та модулі, обробляється як об'єкти. Це відбувається за рахунок швидкості, але значно полегшує написання розширеного коду. Розробники можуть виконувати складні маніпуляції з об'єктами лише за допомогою кількох інструкцій і навіть розглядати частини програми як абстракції, які при необхідності можуть бути змінені.

5.3 Бібліотека OpenCV

Бібліотека OpenCV була обрана для коректної роботи із зображеннями. OpenCV (Open Source Computer Vision Library) - це бібліотека програмного забезпечення для комп'ютерного зору та машинного навчання. OpenCV був спрямований на забезпечення спільної інфраструктури для програм комп'ютерного зору та прискорення використання машинного сприйняття. Бібліотека містить понад 2500 оптимізованих алгоритмів, включаючи повний набір класичних і передових алгоритмів комп'ютерного зору та машинного навчання. Ці алгоритми можна використовувати для виявлення та розпізнавання облич, розпізнавання об'єктів, класифікації поведінки людей у відео, відстеження руху камери, відстеження рухомих об'єктів, вилучення 3D-моделей об'єктів, створення 3D-хмар точок із стереокамер, пошуку подібних зображень із баз даних зображень, видалення червоного -очі у флеш-зображеннях, відстежуйте рух очей, розпізнавайте пейзажі та встановлюйте маркери для накладання на доповнену реальність тощо.

OpenCV написаний власною мовою на C ++ і має шаблонний

інтерфейс, який безперебійно працює з контейнерами STL. Також бібліотека має інтерфейси C++, Python, Java та MATLAB та підтримує Windows, Linux, Android та Mac OS. У роботі було використано Python інтерфейс цієї бібліотеки.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було розглянуто та порівняно декілька алгоритмів біометричної ідентифікації за обличчям, відбитком пальця та райдужною оболонкою ока, а також обрано алгоритми для оптимізації. Під час порівняння методів зазначених в роботі було детально досліджено всі етапи ідентифікації біометричних характеристик, для виявлення можливих варіантів покращення, починаючи від попередньої обробки зображення, та закінчуючи порівнянням ідентифікаторів знайденими на зображенні з тими, що збережені у системі. Модифікації алгоритмів були спрямовані на покращення таких показників як швидкодія та точність розпізнавання.

Під час виконання роботи були поставлені та виконані такі завдання:

- виконано аналіз сучасних методів розпізнавання обличчя;
- виконано аналіз сучасних методів ідентифікації за відбитком пальця;
- виконано аналіз сучасних методів ідентифікації за оком;
- визначено можливі методи покращення алгоритмів ідентифікації;
- виконано оптимізацію LBP алгоритму, що використовується для ідентифікації особи за обличчям;
- виконано оптимізацію алгоритму ідентифікації за відбитком пальця, шляхом покращення зображення відбитка;
- виконано покращення алгоритма Хафа, що застосовується на етапі локалізації райдужної оболнки ока.

В кінцевому результаті алгоритми біометричної ідентифікації, які були оптимізовані шляхом модифікації певних етапів розпізнавання біометричних ознак, повністю задовільняють наданим вимогам і сформульованим завданням

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Simon Dr. Computer Vision: Models, Learning, and Inference / Dr. Simon, JD Prince[Текст] – California: O'Reilly Media. 2012 – 318 с
2. Prateek J. Artificial Intelligence with Python / J. Prateek [Текст] – California: O'Reilly Media. 2017 – 284 с.
3. An improved face recognition algorithm and its application in attendance management system [Електронний ресурс] / ScienceDirect. – Режим доступу: [www/URL: https://www.sciencedirect.com/science/article/pii/S2590005619300141](http://www.sciencedirect.com/science/article/pii/S2590005619300141) – 17.03.2020 р. – Загол. з екрану..
4. P. Viola and M.J. Jones Robust real-time face detection [Текст] - International Journal of Computer Vision, vol. 57, no. 2, 2004 - 137с.
5. Introductory Chapter: On Fingerprint Recognition. [Електронний ресурс] /IntechOpen. – Режим доступу: [www / URL : https://www.intechopen.com/books/9905](http://www.intechopen.com/books/9905) – 10.02.2021 р. – Загол. з екрану
6. M. Turk, A. Pentland Face recognition using eigenfaces [Текст] - Conference on Computer Vision and Pattern Recognition, 1999 – 586 с.
7. Bradsky G., Kaehler A. Learning OpenCV [Текст] — California: O'Reilly Media, 2008. — 580 с.