Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФКАЦІЙНА РОБОТА

на тему: «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації»

08-20.МКР.014.00.000 ПЗ

Виконав: студент 2 курсу, групи 1БС-21м
спеціальності 125 Кібербезпека
_____ Кулик Л. Р.

Керівник: к. т. н., проф. каф ЗІ
_____ Кондратенко Н. Р.
«13» грудня 2022 р.

Опонент: к. т. н., доц., доц. каф. ПЗ
_____ Катєльніков Д. І.
«13» грудня 2022 р.

Допущено до захисту

Завідувач кафедри ЗІ, д.т.н., проф
_____ Лужецький В. А.
«13» 12 2022 р.

Вінниця – 2022 р.

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 «Інформаційні технології»
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д.т.н, проф.
_____ В. А. Лужецький
«01» 09 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Кулику Леоніду Руслановичу

1. Тема роботи: «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації» керівник роботи: Кондратенко Наталія Романівна, к. т. н., проф. каф. ЗІ, затверджені наказом ректора ВНТУ від 14 вересня 2022 року №203.

2. Строк подання студентом роботи: 19 грудня 2022 р.

3. Вихідні дані до роботи:
   – операційна система розробки – Windows;
   – розробка ізольованих модулів для ідентифікації користувача;
   – середовище розробки – Visual Studio Code;
   – мова програмування – Python;

4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Побудова моделей ідентифікації обличчя. 3. Реалізація та аналіз системи ідентифікації обличчя користувача. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.

5. Перелік графічного матеріалу: Схема загальної структури моделі ідентифікації користувача за обличчям (плакат, А4). Схема процесу отримання вектора унікальних характеристик (плакат, А4). Схема проведення перевірки зображень користувача в процесі роботи (плакат, А4). Структура моделі ідентифікації обличчя користувача (плакат, А4). Діаграма вихідного вектору характеристик користувача для моделі на вузлових точках (плакат, А4). Графік залежності показників FAR та FRR від кількості помилок при ідентифікації (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Кондратенко Н.Р., к.т.н., проф. каф. ЗІ		
2	Кондратенко Н.Р., к.т.н., проф. каф. ЗІ		
3	Кондратенко Н.Р., к.т.н., проф. каф. ЗІ		
4	Лесько Олександр Йосипович к.е.н., доц, професор кафедри ЕПВМ		

7. Дата видачі завдання 1 вересня 2022 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Зміст етапу	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2022 – 04.09.2022	
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	05.09.2022 – 15.09.2022	
3	Науково-технічне обґрунтування	16.09.2022 – 22.09.2022	
4	Розробка технічного завдання	23.09.2022 – 04.10.2022	
5	Аналіз та формування вимог до ПЗ	05.10.2022 – 16.10.2022	
6	Розробка рішень, моделей, алгоритмів	17.10.2022 – 14.11.2022	
7	Тестування розробленого ПЗ	15.11.2022 – 17.11.2022	
8	Розробка розділу економічного обґрунтування доцільності розробки	18.11.2022 – 21.11.2022	
9	Аналіз виконання ТЗ, висновки	22.11.2022 – 24.11.2022	
10	Оформлення пояснювальної записки	25.11.2022 – 29.11.2022	
11	Перевірка магістерської роботи на наявність плагіату	30.11.2022 – 02.12.2022	
12	Попередній захист та доопрацювання МКР	07.12.2022 – 19.12.2022	
13	Представлення МКР до захисту, рецензування	20.12.2022 – 21.12.2022	
14	Захист МКР	22.12.2022 – 26.12.2022	

Студент _____ Кулик Л. Р.
(підпис)

Керівник роботи _____ Кондратенко Н. Р.
(підпис)

АНОТАЦІЯ

УДК 681.325.5

Кулик Л. Р. Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2022. 101 с.

На укр. мові. Бібліогр.: 51 назв; рис.: 32; табл. 17.

Магістерська кваліфікаційна робота присвячена розробці моделей та методів для детекції та ідентифікації обличчя користувачів комп'ютерних систем. В рамках даної роботи було проведено аналіз існуючих моделей та методів біометричної ідентифікації, порівняно існуючі підходи та проаналізовано переваги та недоліки кожного з них. На основі проаналізованих даних було запропоновано удосконалену систему для детекції та ідентифікації обличчя користувачів комп'ютерних систем.

Ілюстративна частина складається з 6 плакатів з демонстрацією результатів розробки і проведених досліджень

В економічному розділі здійснено оцінку витрат на розробку інформаційної технології.

Ключові слова: інформаційна безпека, біометрична ідентифікація, нейронна мережа.

ABSTRACT

Kulyk L. R. Models and methods for detection and identification of faces of computer users. Part 2. Identification module. Master's thesis on specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2022. 101 p.

In Ukrainian language. Bibliographer: 61 titles; fig.: 32; tabl. 17.

The master's qualification work is devoted to the development of models and methods for the detection and identification of the faces of users of computer systems. As part of this work, the existing models and methods of biometric identification were analyzed, the existing approaches were compared, and the advantages and disadvantages of each of them were analyzed. On the basis of the analyzed data, an improved system for the detection and identification of the faces of computer system users was proposed.

The illustrative part consists of 6 posters with a demonstration of the results of development and conducted research

In the economic section, an assessment of costs for the development of information technology was made.

Keywords: information security, biometric identification, neural network.

ЗМІСТ

ВСТУП

Вирішення проблеми захисту корпоративних та приватних даних в наш час виходить за межі прямої взаємодії з користувачем системою ідентифікації. Це в першу чергу пов’язано з переходом більшої частини шуканої та збереженої інформації в цифровий формат. Дані особливості сформували нові потреби в етапах розробки і імплементації механізмів в захисті даних.

В запропонованій системі ідентифікації обличчя користувачів комп’ютерних систем лежать в основі технології нейромережевого підходу, які надають можливість ідентифікації користувачів на основі індивідуальних антропометричних візуальних показників вказаного суб’єкта, з метою запобігання злиття даних, та для ідентифікації невизначених або злочинних суб’єктів.

Велика популярність інтернету речей пов’язана в основному з тим, що він дозволяє отримати потрібну інформацію у будь-який час доби та у будь-якому місці, а найголовніше є те, що це дозволяє людям спілкуватись незалежно від їх географічного розташування. Тому, аби полегшити долю сучасного користувача комп’ютерних систем, ведуться розробки сучасних біометричних технологій та методів для ідентифікації користувача, для покращення інфраструктури розмежування доступу різних суб’єктів для доступу до інформації різного рівня доступності.

В цілому біометрія – це наука, яка вивчає можливість ідентифікації кожної конкретної людини за різними характеристиками людського тіла, будь то відбитки пальців або унікальні властивості зіниць або голосу людини. Використання біометричних методів ідентифікації в більшій мірі відсіює всі інші наявні методи ідентифікації, такі як унікальні найменування, чи цифрові номери, які людина може забути, в випадку з біометричними методами такого відбутись не може. Сьогодні більшість підприємств використовують передові системи контролю та управління доступом. Адже завдяки існуючим біометричним системам можна значно підвищити безпеку доступу до інформаційних ресурсів.

У минулому розмежування доступу та ідентифікація користувачів, проводилась встановленням пропускних пунктів зі сканерами карток чи відбитків пальців, але на сьогоднішній день, в зв’язку зі швидким розвитком біометричних технологій, підприємства все частіше звертаються до інших більш точних і зручних методів ідентифікації. Наприклад, ідентифікація обличчя користувача у відео потоці.

Змусити комп’ютер бачити – це складне завдання, яке вписується в концепцію використання штучного інтелекту, який націлений на імітацію різних видів діяльності, чи відтворення стану роботи людини. Головними аспектами в розробці є алгоритми обробки зображень, а саме статичні та рухомі. Тому в основному це підходить для ідентифікації користувача на основі антропометричних показників геометрії тіла користувача, а саме обличчя.

Об’єктом дослідження є ідентифікація обличчя користувачів.

Предметом є моделі та методи ідентифікації обличчя користувача за біометричними характеристиками.

Метою магістерської кваліфікаційної роботи є вдосконалення існуючих моделей та методів ідентифікації обличчя користувача на базі нейронних мереж.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

– дослідити існуючі методи ідентифікації користувача;

– дослідити існуючі моделі для ідентифікації обличчя користувача;

– реалізувати моделі ідентифікації на основі отриманої інформації;

– розробити модель інформаційної технології;

– розробити алгоритми функціонування інформаційної технології;

– обрати засоби реалізації програмного засобу;

– визначити економічну доцільність від розробки засобу детекції та ідентифікації обличчя користувача;

– реалізувати програмний засіб на основі розроблених моделей, алгоритмів та обраних засобів.

Наукова новизна роботи полягає в наступному: запропоновано алгоритм розпізнавання обличчя користувача, що поєднує методи екстракції унікальних

характеристик з використанням прихованого коду кодувальної нейронної мережі та нормалізацію зображення; виділено 3 опорні вектори орієнтирів для ідентифікації та локалізації особливих рис обличчя, що є основою для подальшої обробки зображення обличчя; зважаючи на результати, що для центросиметричного оператора було змінено оптимальний розподіл зображення та покращено з точки зору споживання пам’яті та ефективності розпізнавання.

Практична цінність полягає у тому, що розроблено застосунок, має можливість бути використаним як система в корпоративних умовах для запобігання витоку даних та виявлення злочинних суб’єктів. Низьке ресурсоспоживання розробленої системи ідентифікації обличчя користувача полегшує застосування розробленого алгоритму у високонавантажених системах з великою кількістю користувачів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз існуючих методів ідентифікації

Автентифікація є одним із найбільш перспективних способів підвищення довіри та безпеки для комерційних програм, так як дозволяє відповісти на питання, хто є користувачем і чи дійсно користувач є тим, за кого себе видає, також позначає властивість забезпечення ідентичності попередньо згаданих сутностей. Крім того, авторизація – це процес надання окремим особам доступу до системних об’єктів на основі їх ідентифікації.

«Ідентифікація», «автентифікація» та «авторизація» – це три взаємопов’язані поняття, які утворюють ядро системи безпеки [1].

Ідентифікація – це передача ідентифікаційної інформації до інформаційної системи (ІС). Перед автентифікацією заявник зазвичай надає ІС інформацію про особу, а далі вже відбувається процес підтвердження особи шляхом автентифікації, тобто заявник підтверджує особу шляхом автентифікації, наприклад, за допомогою пароля.

Автентифікація – це доказ, наданий позивачем, щоб підтвердити, що позивач дійсно відповідає наданій особистості.

Авторизація – це надання користувачеві привілеїв.

Останнім часом захист даних стає дедалі складнішим завданням. Компанії та організації вживають заходів для захисту своїх активів, а методи ідентифікації стають все більш важливим заходом безпеки. Традиційно механізми ідентифікації поділяються на такі категорії [2]:

- на основі фактору знань;
- на основі фактору володіння;
- на основі фактору приналежності.

Ідея методів ідентифікації на основі фактору знань полягає в тому, що користувач знаєте секрет, який часто називають паролем, який не знає ніхто

інший. Таким чином, знання секрету відділяє його від усіх інших користувачів ІС.

Використання секрету має наступні недоліки: якщо секрет вводиться за допомогою набору на клавіатурі, то існує імовірність, що зловмисник зможе підглянути секрет; люди, як правило, вибирають паролі, які легко запам’ятати, що зазвичай означає, що пароль можна легко вгадати; зміна пароля вимагає втручання людини, таким чином, зламані паролі можуть залишатися дійсними довше, ніж бажано.

Методи ідентифікації на основі фактору володіння вимагають від користувача надати докази володіння ним фізичним об’єктом, наприклад:

- SIM-картка;
- мобільний телефон;
- смарт-карта;
- апаратний OTP-токен;
- ключ безпеки FIDO2.

Фактор володіння перевіряє, чи є у користувача відповідне апаратне забезпечення для ідентифікації, що робить його набагато важчим зламати, ніж фактор знань. Зловмисник може спробувати здійснити успішну атаку, отримати віддалений доступ до частини обладнання або навіть викрасти цю частину обладнання. Тим не менш, зробити будь-яке з цього складніше, ніж виконати просту атаку підбору секрету грубою силою чи за допомогою методу «словник». Дані методи є більш безпечнішими в порівнянні з методами на основі фактору знань, тому для збільшення міцності системи безпеки зазвичай комбінують ці 2 фактори.

Методи ідентифікації на основі фактору приналежності часто називають найсильнішим з усіх факторів ідентифікації [3]. Фактор приналежності просить користувача підтвердити свою особу, надавши докази, властиві тільки йому унікальні характеристики. Ці характеристики мають досить легко та швидко зчитуватись, і бажано, щоб це були речі, які важко підробити, наприклад:

– сканування сітківки;
– сканування обличчя;
– сканер відбитків пальців;
– зчитувач відбитків рук;
– голосовий друк;
– динаміка набору на клавіатурі;
– динаміка руху при підписі.

Для реалізації схеми біометричної ідентифікації зберігається деяке представлення характеристики, що цікавить. Під час ідентифікації користувача відбувається нове вимірювання характеристики та порівнюється з тією, що була збережена. Точного збігу не очікується, і його не повинно бути через рівень помилок, пов’язаних із біометричними датчиками та методами/моделями, які використовуються для екстракції характеристик.

Хоч біометрія і забезпечує найнадійнішу ідентифікацію, вона чутлива до помилок. Помилка першого роду виникає, під час відхилення наявного користувача та показує, що користувач невідомий. Помилка другого роду, під час помилкової ідентифікації невизначного користувача як наявного користувача. Біометричні системи, як правило, можна налаштувати на чутливість, але чутливість впливає на точність роботи системи. Дані недоліки нівелюються тим, що ідентифікація буде проводитись неперервно, тому є можливість знизити чутливість системи, тому для вирішення задачі неперервної ідентифікації, методи біометричної ідентифікація підходять найкраще.

Біометрична ідентифікація в порівнянні з іншими методами має суттєві переваги [4], такі як:

– швидка ідентифікація. За допомогою біометрії користувач має можливість бути швидко авторизованим;

– зручність. Використання біометричних технологій, надає можливість зберігати дані про відвідування співробітників у базах даних. Далі ці дані можна легко переглядати, оновлювати та шукати невідповідності;

– масштабованість. Біометричні функції можна використовувати для багатьох проектів і задач;

– унікальність характеристик як базис методу. Біометрія дає контроль доступу менеджеру. Біометричний відбиток пальця та обличчя неможливо викрасти та не піддаються віддаленому зламу, авжеж в випадку стійкості самих систем, які пов’язані з датчиками зчитування характеристик користувача;

Біометричну ідентифікацію можна підсумувати двома етапами, а саме реєстрацією та автентифікацією [5]. На етапі реєстрації користувач надає свої біометричні дані. Біометричні дані зчитуються, відбувається екстракція характеристик користувача та результат зберігається до бази даних. Під час процесу ідентифікації збережені функції порівнюватимуться з тими, які зараз представлені для доступу. Якщо вони збігаються, чи знаходяться на короткій дистанції один від одного, тоді користувачу буде надано доступ.

1.2 Аналіз методів біометричної ідентифікації

Для біометричної ідентифікації підходить практично будь-яка фізіологічна особливість; однак найбільш узагальнені біометричні методи включають [6]: автоматизоване розпізнавання відпечатків пальцівві, сітківки, геометрії руки, обличчя, голосу, райдужної плівки ока, та підпису. Підвищена обізнаність щодо питань безпеки призвела до масового зростання інтересу до біометричних технологій з боку різноманітних ринкових секторів, включаючи державні установи та корпорації, які прагнуть посилити підзвітність свого персоналу та підвищити рівень безпеки для їх приміщень.

Прогнози галузі вказують на те, що загальний ринок біометрії продовжуватиме зростати, досягнувши до 2025 року 35 мільярдів доларів доходу [7] (рис. 1.1).

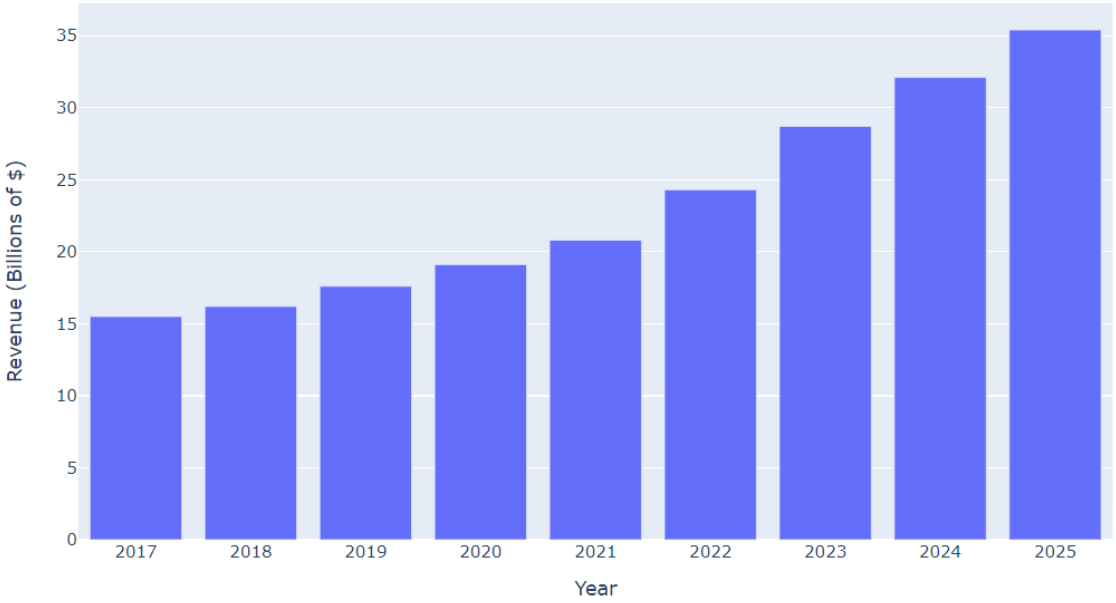


Рисунок 1.1 – Загальний ринок доходів від біометрії: 2017 – 2025 роки

Що стосується різних використовуваних біометричних технологій, відбиток пальця та портрет обличчя продовжують залишатися провідними технологіями з точки зору частки ринку [7] (рис. 1.2).

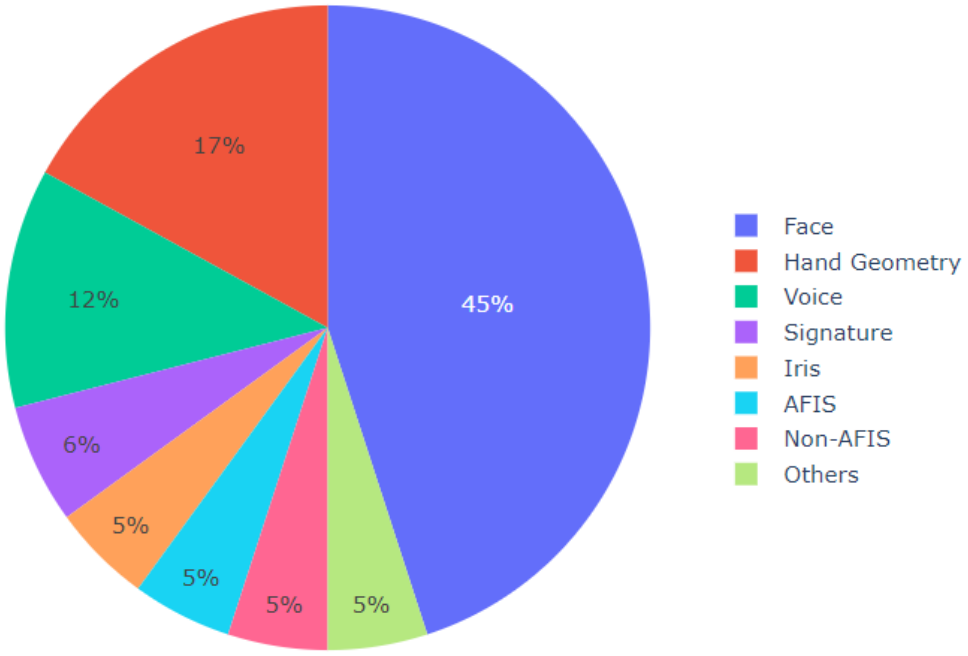


Рисунок 1.2 – Частка ринку біометрії за технологіями в 2017 році

Загалом біометричні методи можна розглядати як автоматичні системи розпізнавання образів, які встановлюють автентичність певної фізіологічної або поведінкової характеристики, якою володіє користувач [8]. На першому етапі

реєстрації (навчання системи) система фіксує індивідуальні фізіологічні характеристики, які можуть бути представлені за допомогою векторних шаблонів ознак або прототипів. Найчастіше етап реєстрації охоплює весь термін служби системи, оскільки можна очікувати нових користувачів. Після цього окремі користувачі отримують доступ до системи, яка зможе фіксувати їхні біометричні характеристики, створює цифрове представлення та порівнює його з шаблонами, що зберігаються в базі даних, щоб прийняти рішення щодо особи користувача.

Біометричні методи ідентифікації можуть працювати двома різними способами: в режимі верифікації та ідентифікації. У режимі верифікації користувач видає себе за когось і система просто приймає або відхиляє запит користувача після порівняння біометричних характеристик з тими, що зберігається в базі даних. У режимі ідентифікації користувач поєднується до процесу ідентифікації, який витягує біометричні характеристики користувача та порівнює їх із всіма іншими в базі даних, щоб визначити, чи є цей користувач серед усіх зареєстрованих. Очевидно, що ідентифікація є набагато більш вимогливою, ніж верифікація, по-перше, тому що потрібно виконати більшу кількість порівнянь, а по-друге, тому що таким чином зростає загальна ймовірність похибки [9]. Найбільш поширені біометричні технології та їх ефективність з точки зору практичних питань, класифікованих у широких термінах наведено у таблиці 1.1 [10].

Методи біометричної ідентифікації поділяться на дві групи [11]: Статичні методи та динамічні методи. Статичні методи ґрунтуються на фізіологічних характеристиках людини, до таких методів відносяться:

- портрет обличчя;
- відбитки пальців;
- геометрична будова руки;
- райдужна плівка ока;
- сітківка ока.

Таблиця 1.1 – Основні характеристики біометричних методів ідентифікації

Метод отримання біометричних параметрів	Зразок	Досліджувані риси	Складність в використанні	Ймовірність відмови у доступі %	Вартість у.о.
Портрет обличчя	Зображення особи	Умовне розташування, розташування вилиць та носова форма	Низька	1 – 9	5500
Відбитки пальців	Зображення відпечатку пальців	Розміщення та напрям гребінчастих виступів і розгалужень на відпечатку пальців	Низька	2 – 6	Від 60 до 600
Геометрична побудова руки	Тривимірне зображення зверху та боків кисті	Висота та ширина суглобів, кісток та пальців	Середня	0.7 – 4	Від 600 до 3000
Райдужна плівка ока	Зображення райдужної плівки ока	Смужки і борозенки на райдужній плівці ока	Висока	0.2 – 5	Від 500 до 6000
Сітківка ока	Зображення сітківки ока	Шар кровоносних судин	Висока	0.8 – 3	Від 1500 до 9000
Підпис	Динаміка руху ручкою для введення	Час, динаміка, прискорення на окремих ділянках	Висока	0.5 – 11	Від 300 до 1500
Голос	Запис голосу	Частота, модуляція та тривалість голосового виду	Середня	–	–
Рух роботи з клавіатурою	Ритм машинопису	Зватримки, час переходу з однієї клавіші на іншу	Середня	3 … 9	–

Розглянемо детально кожен з вказаних методів окремо.

Ідентифікація по портрету обличчя. В цьому методі ідентифікації формується трьохвимірний образ людського лиця. На ньому визначаються контури основних рис обличчя, відстань між ними розраховується і створюється не просто плоский вигляд, а ще велика кількість видів на кшталт випадків, коли повертають голову або нахиляють, а також при зміні виразу обличчя. Недоліком даного методу є те, що в більшості випадків неможливо охопити всі варіанти нахилу голови, що може призвести до неправильної ідентифікації користувача.

Ідентифікація за допомогою відбитків пальців будується на унікальності малюнка папілярного візерунку пальців людини. Одержаний відбиток за

допомогою сканера, перемінюється в цифровий код, який залишається в базі даних, а потім порівнюється з раніше залученими для ідентифікації особи. До переваг ідентифікації за допомогою відбитка пальців відносять: зручне та неважке використання і надійність, висока точність і низько вартісні пристрої для сканування. Також наявні такі недоліки: змінення папілярного візерунка невеликими ранками, подряпинами, хімічні опіки; неможливість зчитування суха шкіра, що не дозволяє деяким сканерам зчитувати відбиток.

Ідентифікація за геометричною будовою руки відбувається за допомогою спеціальних пристроїв, які складається з камери і декількох діодів, які при включенні по черзі можуть фіксувати різні проекції долоні, за допомогою чого в свою чергу відбувається побудова тривимірного образу структури руки користувача за яким формується згортка і стає можливим розпізнавання людини. Перевагою даного методу над ідентифікацією за відбитком пальця є більша точність, а недолім є великий за розмір та ціна сканера.

Ідентифікація за райдужною плівкою ока будується на факті унікальності малюнку райдужної плівки ока особи. Щоб її відсканування, буде достатньо портативної камери зі спеціалізований програмним забезпеченням, яке може вміщати зображення особи, з виділенням зображення ока, яке одразу виділяє малюнок райдужної плівки, за допомогою якого створюється цифровий код для ідентифікації. Недоліком даного методу ідентифікації є менша точність в порівнянні з іншими методами, це пов’язано в першу чергу з меншим числом унікальних параметрів особи, які можна отримати з сітківки ока.

Ідентифікація за розпізнаванням сітківки. Методи ідентифікації на базі сітківки аналізують шар кровоносних судин, розташованих у задній частині ока. Ця технологія вважається високоточною технологією. Для захоплення візерунків сітківки ока використовується джерело інфрачервоного світла, а потім візерунок аналізується на предмет характерних точок, які формують виразкову інформацію.

Динамічні методи базовані на різноманітті людських дій - підсвідомих змін положень базових рис в процесі виконання якої-небудь дії. В порівнянні з

статичними методами, динамічні – більш простіші в реалізації, тому що зазвичай для них не використовується дороге обладнання. Можна обмежитись лише програмним забезпеченням, воно також вимагає мінімум втручання фахівця. До таких методів відносять:

- голос;
- підпис;
- динаміка роботи з клавіатурою;

На особливих характеристиках мови базується ідентифікація за голосом, ці характеристики виникають через анатомічні особливості форм рота та горла, будови голосових зв'язок, розмірів та через набуті звички, такі як звучання, гучність, швидкість. Як недолік можна визначити такі фактори, які мають вклад на результати розпізнавання: завади в мікрофоні, навколишнє оточення на результати розпізнавання наприклад шуми, помилки при проголошенні, різний емоційний стан, а також використання різної якості пристроїв для реєстрації при записі еталонів та ідентифікації користувача та перешкоди в низькоякісних каналах передачі даних тощо.

Ідентифікація за підписом відбувається за підписом особи (або кодового слова). Цифровий код ідентифікації формується за динамічними характеристикам письма, тобто для ідентифікації будується згортка, в яку входить інформація: безпосередньо інформація про підпис, часові характеристики надання підпису і статистичним характеристики динаміки натиску на поверхня. Недоліком даного методу є те, що потрібні спеціалізовані засоби реєстрації динаміки введення підпису.

Ідентифікація за динамікою роботи з клавіатурою базується на факті того, що клавіатурний почерк користувача є стабільною характеристикою. Недоліком даного методу ідентифікації є те, що його застосування доцільно тільки по відношенню до користувачів з досить довгим досвідом роботи. Тому з іншими ймовірність хибного розпізнавання справжнього високо підіймається та робить неможливим цей спосіб для використання на практиці.Виходячи з теорії

машинопису і діловодства можна дізнатися час появи почерку роботи з клавіатурою, при якому досягається необхідна ймовірність ідентифікації користувача: приблизно 6 місяців [6]. Даний недолік також можна обійти, розробивши модель динамічного підлаштовування клавіатурного почерку користувача до еталонного екземпляру.

Всі вище перелічені методи ідентифікації, як статичні, так і динамічні об’єднує те, що вони використовуються для одноразової ідентифікації користувачів, для надання їм в подальшому певних прав. Цей факт може стати причиною викрадення або незаконного проникнення до даних вже через попередньо автентифіковану особу. Наприклад користувач скористався одним з представлених методів ідентифікації, система визначить його та надає відповідні права, але в цей момент керування над системою може перехопити зловмисник, скориставшись необачністю або халатністю співробітника. Наприклад, це може статись в період відсутності власника системи. Для передбачення такої загрози потрібно забезпечити можливість використання даних методів в режимі безперервного моніторингу та безперервної ідентифікації.

Тобто, для вирішення задачі ідентифікації в режимі моніторингу, підходять лише 2 методи: динаміка роботи з клавіатурою та за портретом обличчя.

В даній роботи використовується метод безперервної ідентифікації за портретом обличчя. Принцип роботи методу наступний – в певні проміжки часу через відбувається зчитування користувача через об’єктив, даний процес ніяк не залежить від користувача, далі на зображенні відбувається виділення лиць наявних осіб, з виділених зображень відбувається процес екстракції характеристик, потім відбувається порівняння отриманих характеристик з тими, що є наявні в базі. Якщо характеристики збігаються, чи мають досить малу відстань один від одного – користувач вважається таким, що є автентифікованим, інакше відбувається процес де ідентифікації та блокування системи з пропозицією ввести пароль. Перевагами даного методу є його точність та безперервність роботи, тобто він не залежить ні від чого іншого, окрім заданої

частоти проходження користувачем ідентифікації. Одним з суттєвих недоліків методу є те, що камера користувача має бути завжди під’єднана до системи та направлена на нього.

1.3 Аналіз існуючих моделей та методів ідентифікації за портретом обличчя

Головною перевагою систем розпізнавання обличчя є їх зручність автоматичного розпізнавання, оскільки це здається для користувача більш природнім в порівнянні з іншими методами ідентифікації. Використання розпізнавання обличчя включає багато засобів використання, таких як обмеження доступу до зон, відеоспостереження, додатки для правоохоронних органів тощо. Враховуючи різноманіття засобів використання, відповідно були розроблена низка різних методів для розпізнавання обличчя, також було раніше проаналізовано те, як люди впізнають один одного, дана інформація може бути корисною для розробки систем автоматичного розпізнавання обличчя [12].

Розпізнавання обличчя можна здійснювати за нерухомими зображеннями, відеорядами, стереозображеннями, зображеннями діапазону тощо. На сьогоднішній день існує безліч алгоритмів для розпізнавання обличчя починаючи від фільтрації Габора до генетичних алгоритмів [12].

Однією з перших робіт з комп’ютерного розпізнавання обличчя є метод побудований на локалізації ряду точок на обличчі та визначенні їх відстаней, тобто характеристик обличчя з точки зору відстаней та кутів між точками, такими як кут очей, кінцівки рота тощо. Враховуючи даний набір відстаней до користувача застосовують методи класифікації, які використовуються для ідентифікації особи.

Використання статистичних підходів для розпізнавання обличчя є більш новим підходом [13]. Для цього використовується розкладання Карунена-Лоева, щоб отримати набір власних векторів, відомих як власні грані. Тоді будь-яке зображення можна представити за допомогою зваженої комбінації даних граней. Вагові коефіцієнти отримують шляхом проектування зображення на компоненти

власних граней за допомогою операції внутрішнього добутку. Ідентифікація зображення відбувається методом пошуку зображення в базі даних, розмірність якого є найближчими за евклідовою відстанню, до ваг тестового зображення. Для перевірки зображення необхідно застосувати порогове значення, враховуючи евклідову відстань між тестовим і еталонним представленням на основі власного обличчя, вважаючи, що обличчя належить справжньому користувачеві, якщо відстань менша за зазначену. Важливо зауважити, щ реєстрація положення та розміру обличчя необхідна для досягнення стійкості щодо отримання зображення [14]. В даному методі система застосовує перетворення Фур'є до стандартизованого зображення та використовує отриманий спектр Фур'є замість просторових даних для розширення перетворення власних векторів.

SVM класифікатор є досить популярним методом для розпізнавання обличчя [15]. Оскільки розпізнавання обличчя є в повній мірі проблемою класифікації з кількістю класів K, де K – кількість відомих користувачів. Тоді проблема розпізнавання обличчя може бути переформульована як проблема класифікації двох класів, де класи – це відмінності між обличчями однієї людини, і відмінності між обличчями різних людей. Зображення обличчя можна представити у вигляді вектора з розмірністю N. Вектор може бути як комбінація пікселів зображення, як метричні характеристики обличчя виражена як комбінація власних граней. Цікавим є використання SVM класифікатора з точки зору класифікації з кількістю класів K рівним одиниці, тобто проведення тренування тільки для однієї особи з можливістю використання отриманої моделі як детектор аномалій чи відхилень від тих значень що належать користувачу.

Використання нейронних мереж є одним з найпопулярніших методів для розпізнавання обличчя [16]. Ряд систем використовує нейронні мережі не тільки для розпізнавання обличчя, але й для класифікації статі та виразу обличчя користувача. Використання нейронних мереж є альтернативою використанню інших класифікаторів після отримання вектора ознак. Також необхідно зауважити, що локалізацію точок на обличчі також можна робити за допомогою

нейронних мереж, таким чином можна побудувати комплексну систему, яка буде складатись з декількох нейронних мереж. За допомогою нейронних мереж можливо зробити екстракцію характеристик користувача з зображення, та провести порівняння отриманих характеристик з тими, що збережені в базі, на основі чого прийняти рішення про ідентифікацію.

В максимально спрощеному вигляді будь-яка система біометричної ідентифікації за розпізнаванням обличчя буде мати вигляд як на рис. 1.3.

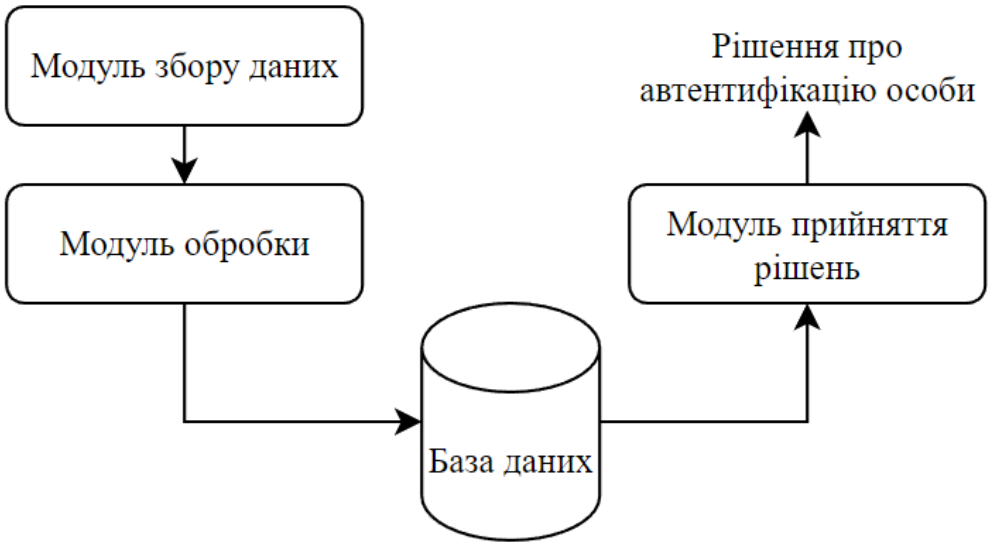


Рисунок 1.3 – Загальний вигляд моделі для біометричної системи

Тобто є 3 основних модулі структури роботи системи:

– модуль збору даних;
– модуль обробки;
– модуль прийняття рішень.

Модуль збору даних. Ця підсистема відповідає за фіксацію біометричних ознак, що підлягають аналізу. На даному етапі відбувається створення знімку користувача та виділення його від фону.

Модуль обробки. Даний модуль є найважливішим в усій системи, так як в ньому визначаються моделі та методи для екстракції характеристик користувача.

Найпопулярнішими на сьогоднішній день є нейромережеві методи екстракції характеристик, такі як:

– згорткові нейронні мережі – це алгоритм глибокого навчання, який може приймати на вхід зображення, призначати ваги та зміщення, які отримуються шляхом навчання, різним аспектам чи об’єктам зображення та має можливість розрізняти зазначені класи один від іншого [17]. Перевагою даного методу є те, що ми можемо використати увесь багаж «знань», конкретної згорткової нейронної мережі для екстракції вектора характеристик, попередньо прибравши класифікаційний шар з кінця мережі, таким чином є можливість адаптувати мережу під нову задачу, яка виключена з рамок звичайної класифікації;

– автокодувальники – це тип нейронних мереж прямого зв’язку, де вхідні дані збігаються з вихідними [18]. Даний тим нейронних мереж стискають вхідні дані в вектор меншої розмірності – код, а потім реконструюють вихідні дані з цього представлення. Код є компактним «підсумком» або «стисненням» вхідних даних, що також називається представленням прихованого простору. Мережа складається з 3 компонентів: кодувальника, коду та декодувальника. Кодувальник стискає вхідні дані та створює код, декодувальник потім реконструює вхідні дані лише за допомогою цього коду. Перевагою даного методу є те, що кодувальник та декодувальник є автономними моделями, що дозволяє використовувати їх незалежно один від одного. Тому кодувальник представляє досить велику цікавість з точки зору представлення прихованого простору, який можна використати як вектор унікальних характеристик користувача для розпізнавання обличчя;

– детекція вузлових точок – це одне з ключових завдань комп’ютерного зору, в якому модель має передбачити ключові точки, що представляють області або орієнтири на обличчі людини – очі, ніс, губи тощо [19]. Виявлення орієнтирів обличчя є базовим завданням, яке можна використовувати для виконання інших завдань комп’ютерного зору, зокрема оцінки пози голови, визначення напрямку погляду, визначення жестів обличчя тощо. Дана технологія дозволяє визначити набір унікальних точок та їх відстаней один від одного, цей набір точок можна

представити в вигляді унікального вектору характеристик користувача, так як в кожної людини набір буде унікальний. Ця особливість може слугувати гарним ідентифікатором користувача для систем біометричної ідентифікації за розпізнаванням обличчя.

В даній роботі кожна з вище представлених моделей буде проаналізована, буде порівняна їх продуктивність, швидкість роботи та точність.

Модуль прийняття рішень. В даному модулі визначаються алгоритми порівняння векторів характеристик користувачів. Від налаштування та вибору даних алгоритмів буде залежати загальна продуктивність всієї системи, тому необхідно впевнитись в доцільності використання обраного методу. Існує 3 основних методи порівняння векторів:

– евклідова відстань – міра відстані, визначається як довжина відрізка, що сполучає дві точки. В основному використовується на маловимірних даних де важливо виміряти величину вектора. Недоліками даної міри відстані є те, що перед використанням необхідно нормалізувати дані. Також зі збільшенням розмірності ваших даних дана міра стає менш корисною, це пов’язано з прокляттям розмірності, яке пов’язане з уявленням про те, що багатовимірний простір не діє так, як інтуїтивно очікується від 2- чи 3-вимірного простору [20];

– схожість за косинусом – це косинус кута між двома векторами. Одним з головних недоліків косинусної подібності є те, що не враховується величина векторів, а лише їх напрямок, це означає, що різниця в значеннях не враховується повністю. В основному використовується, коли наявні багатовимірні дані та коли величина векторів не має значення;

– Manhattan Distance – обчислює відстань між дійсними векторами, так як наче вони можуть рухатися лише під прямим кутом, тобто при обчисленні відстані немає діагонального руху [21]. В основному використовується для даних великої розмірності. Дана міра, дещо менш інтуїтивно зрозуміла, ніж евклідова відстань, особливо при використанні у даних великої розмірності. Також використовується, якщо набір даних має дискретні та/або бінарні атрибути,

оскільки враховує кроки, які реально можуть бути зроблені в межах значень цих атрибутів.

Враховуючи вище перелічені факти, безперервна автентифікація за обличчям користувача з використанням нейронних мереж має значні переваги над усіма іншими моделями та методами, тому було прийнято рішення про втілення в системі саме цього підходу.

Отже, було проаналізовано літературні джерела, які будуть використовуватись у подальшому виконанні кваліфікаційної дипломної роботи. Було проаналізовано основні методи ідентифікації, її види та категорії. Було досліджено методи ідентифікації за допомоги біометрії, досліджено їх види, призначення, було проаналізовано їх техніко економічне обґрунтування. Досліджено придатність кожного з методів біометричної ідентифікації на здатність розпізнавання користувача в безперервному режимі. Проаналізовано методи безперервної автентифікації за обличчям користувача з використанням нейронних мереж та наведено причини використання в даній роботі. Описано алгоритм роботи системи ідентифікації та проаналізовано різні види його реалізації. Аргументовано використання всіх запропонованих методів та засобів для ідентифікації користувача.

2 ПОБУДОВА МОДЕЛЕЙ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧІВ

Процедура розпізнавання обличчя налічує такі кроки [22]:

– розпізнавання обличчя – відбувається незалежно від того, яка постає перед нами задача: ідентифікувати людей за фотографіями, відеорядами чи будь-яким іншим способом;

– позиціонування обличчя – є дуже мало фотографій людей, які стоять прямо обличчям до камери, у більшості випадків обличчя повернене. Таким чином, постає завдання визначити місце розташування обличчя так, якби фотографія була зроблена безпосередньо; позиціонування обличчя – не часто зустрічаються фотографії, на яких людина стоїть прямо обличчям до об’єктива, найчастіше обличчя знаходиться повернуте. Тому виникає завдання позиціонувати обличчя так, ніби фотографія зроблена прямо;

– визначення унікальних рис обличчя – цей крок можна назвати зрілим етапом розпізнавання обличчя (попередній етап є підготовчим). На цьому етапі ми аналізуємо зображення та отримуємо унікальне числове значення для обличчя;

– ідентифікація особи - ми порівнюємо отримані дані з уже наявними, якщо знаходимо схожі дані, то виводимо ім'я людини, якщо ні, то людина нам невідома..

У процесі впровадження необхідно звернути увагу на всі етапи побудови системи розпізнавання обличчя з використанням різних бібліотек, порівняння результатів розпізнавання, отриманих за допомогою цих бібліотек, і визначення швидкості роботи використання різних комп’ютерних бібліотек на кожному етапі глибинного навчання.

Перш за все, необхідно виконати аналіз існуючих методів розпізнавання обличчя та зробити на основі отриманої інформації власний метод. При побудові системи ідентифікації користувача з використанням нейронних мереж,

необхідно враховувати основні характеристики та умови доцільності застосування конкретних архітектурних рішень, такі як:

– параметри вхідних даних;
– вимоги до вихідної інформації;
– апаратні обмеження;
– обмеження часу навчання;
– технічні обмеження нейронної мережі;
– визначення сфери застосування.

Основні вимоги до освітніх даних:

– достатня кількість параметрів, що описуються набором даних;
– кількість прикладів в наборі даних;
– інформативність даних;
– необхідність в підготовці вхідних даних;
– повнота наборів вхідних даних.

Загальні обмеження в процесі навчання нейромережі [23] передбачені таким чином:

– обмеження часу навчання нейромережі;
– тип навчання визначений як з викладачем;
– потреба автоматизації навчальних процесів визначає загальні кількості отриманих параметрів при навчанні;
– впровадження додаткових можливостей навчання під час або після процесу використання;
– вимоги до якості навчання нейромережі, виражені у вибраних показниках - необхідних рівні помилкового розпізнавання.

На практиці вимоги до обладнання визначаються максимальною кількістю прикладів, проаналізованих мережею для досягнення бажаного рівня точності рішень. Точність, у свою чергу, характеризується значеннями максимальної похибки мережі та середньої похибки на реальних даних, які в цілому можуть перевищувати діапазон навчальних даних. Тому завдання полягає в

екстраполяції результатів навчання нейронної мережі за межі навчального набору. Слід зазначити, що обчислювальна потужність, необхідна для розробки моделі, залежить від її типу та алгоритму навчання.

Технічна реалізація ЯМ формує такі обмеження:

Сформовані наступні обмеження щодо технічної реалізації НМ:

– швидкість прийняття рішень;

– інтеграція в існуюче обладнання;

– обсяг та складність реалізація програми.

Сфера застосування визначає спосіб застосування ЯМ. Сьогодні розпізнавання та оптимізація зображень за допомогою NM стало поширеним явищем. Слід зазначити, що системи розпізнавання зображень принципово відрізняються від систем аналізу тексту тим, що їх кількість виходів і комбінацій вхідних параметрів принципово обмежена. У системах аналізу тексту, ця кількість принципово необмежена.

Придатність мережі для автономної роботи визначає діапазон її застосування. Для цього архітектури нейронних мереж повинні забезпечувати можливість повністю автоматизувати процес навчання. Виходячи з матеріалу даної роботи, можна стверджувати, що ключовими завданнями застосування нейронних мереж у сфері програмного забезпечення техніко-економічних систем є:

– розпізнавання образів – включаючи завдання класифікації, кластеризація включає завдання класифікації, кластеризації зображень і апроксимації функцій;

– визначення оптимальної схеми управління – включаючи оптимальні завдання управління та завдання управління еталонної моделі;

– створення асоціативних пам'яток – ей проект включає завдання створення комп'ютеризованих інформаційних систем із пам'яттю, які розглядаються в цьому проекті.

Крім того, область застосування технології залежить від її актуальності в конкретній області та здатності розробленої мережі впоратися з конкретним завданням. Тому проведення тестів на точність та стійкість є критичними для усієї системи.

Розробка біометричних моделей розпізнавання обличчя має багато безсумнівних переваг перед іншими біометричними методами та технологіями:

– не вимагає прямого контакту з особою, чию особу ідентифікує сканер (особі не потрібно залишати відбитки пальців, дивитися на камеру або щось говорити), за винятком систем розпізнавання обличчя, які є частиною стандартних електронних систем безпеки, куди людина під час перевірки дивиться прямо в камеру;

– При наявності відповідного обладнання можна впізнати за рисами обличчя в групі людей на значній відстані і без привернення уваги;

– це єдиний біометричний метод, який не вимагає спеціального обладнання (з використанням стандартних камер відеоспостереження);

– це єдиний біометричний метод з точки зору можливості багатоцільового застосування;

– ідентифікація за допомогою загальнодоступних біометричних даних, які зазвичай не приховані від людини (це важливо урахуванням конфіденційності інших біометричних даних, наприклад, відбитків пальців).

2.1 Моделі ідентифікації обличчя користувачів

Біометрична система розпізнавання обличчя працює точно за алгоритмом, наведеним раніше (див. Розділ 1.1). За допомогою фото- чи відеокамери робиться знімок людини, спеціальним чином обробляється зображення, щоб можна було виділити обличчя в кадрі та оцифрувати його. На отриманому зображенні обличчя виділяється велика кількість індивідуальних параметрів (так звані сторони світу: вилиці, форма очей, перенісся, контур губ тощо).

Існує багато принципово різних підходів для вирішення задачі ідентифікації користувача за обличчям [24], такі як:

– геометричні параметри обличчя;
– порівняння з еталоном;
– нейронні мережі;
– оптичний потік;
– порівняння графів.

Основними критеріями оцінки наведених методів є обчислювальна вартість і надійність розпізнавання побудованих на них алгоритмів.

Для вирішення поставленої задачі найбільш оптимальним рішенням буде використання комбінацій з різних підходів:

– нейромережевий підхід з порівнянням вихідних векторів характеристик моделі [25];
– нейромережевий підхід з використанням кодуючої частини моделей Variational Auroencoders [26];
– нейромережевий підхід для детекції та побудови графу унікальних вузлових точок користувача [27].

В даний час існує близько десятка типів нейронних мереж. Одним із найбільш широко використовуваних варіантів є мережа, побудована на багатошаровому персептроні, що дозволяє класифікувати вхідне зображення/сигнал відповідно до попереднього налаштування/навчання мережі. Нейронна мережа навчається на наборі навчальних прикладів. Суть навчання зводиться до встановлення вагових коефіцієнтів зв'язків між нейронами в процесі вирішення задачі оптимізації за допомогою градієнтного спуску. У процесі навчання НС автоматично виділяються ключові ознаки, визначається їх важливість і будуються зв’язки між ними. Передбачається, що навчена НС здатна застосувати отриманий під час навчання досвід до невідомих образів за рахунок узагальнення.

Найкращі результати в області розпізнавання осіб (за результатами аналізу публікацій) демонструють згорткові нейронні мережі або згорткові нейронні мережі (далі — ЗНМ), що є логічним розвитком подібних ідей НС Машина знань. У порівнянні з багатошаровими персептронами успіх пояснюється можливістю врахування двовимірної топології зображення.

Основними характеристиками мережі є локальні рецепторні поля (забезпечують локальне двовимірне з'єднання нейронів), загальні ваги (забезпечують виявлення певних особливостей будь-де на зображенні) та ієрархічна організація з просторовою підвибіркою. Завдяки цим інноваціям ЗНМ забезпечує часткову стійкість до змін масштабу, зсувів, поворотів, зміни перспективи та інших спотворень. Схематичне зображення архітектури згорткова нейронної мережі зображено на рисунку 2.1.

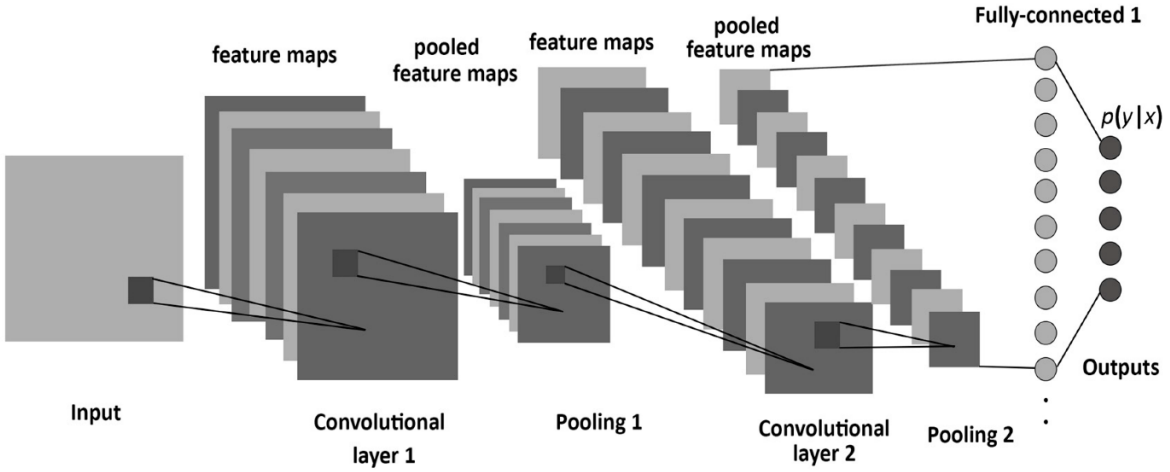


Рисунок 2.1 – Схематичне зображення архітектури згорткова нейронної мережі

Тестування нейромережі на базі даних, яка містить зображення людей з незначними варіаціями в освітленні, масштабі, просторовому обертанні, положенні та різноманітних емоціях, показує точність розпізнавання 96%. Усі особливості архітектури носять закритий характер.

Недоліки нейронних мереж:

– не вимагає прямого контакту з особою, чию особу ідентифікує сканер (особі не потрібно залишати відбитки пальців, дивитися на камеру або щось говорити), за винятком систем розпізнавання обличчя, які є частиною

стандартних електронних систем безпеки, де особа дивиться прямо на особу під час камери процесу перевірки;

– додавання нової референтної людини в базу вимагає повного перенавчання мережі на всій існуючій сукупності (досить тривалий процес, від 1 години до декількох днів, в залежності від розміру вибірки);

– проблеми математичного характеру, пов'язані з навчанням: досягнення локальних оптимумів, вибір оптимального кроку оптимізації та перенавчання;

– етап вибору архітектури мережі (кількість нейронів, шарів, характер зв'язків), що важко формалізується.

У сукупності можна зробити висновок, що НМ є прихованим виконавцем, роботу якого важко розшифрувати. Те, що люди помітно відрізняються зовнішністю, особливо рисами обличчя, очевидно.

Для вирішення задачі ідентифікації користувача з використанням нейромережевого підходу та порівняння вихідних векторів моделі, було обрано архітектуру мережі Inception-ResNet-v1 [28]. Структура даної мережі, а саме залишкові зв’язки дозволяють використовувати ярлики в моделі та дозволили дослідникам успішно навчити ще більш глибокі нейронні мережі, що допомагає покращити продуктивність. Це також дозволило значно спростити початкові блоки.

Найпростіший спосіб покращити продуктивність глибокої нейронної мережі (далі - ГНМ) – це просто збільшити глибину та ширину мережі. Основними недоліками цього методу є збільшення вимоги до кількості даних для подолання можливих обмежень на додатковий обчислювальний ресурс. Фундаментальним способом вирішення цих двох проблем для системи комп’ютерного зору є використання рідкозв’язаної архітектури замість повністю зв’язаної. Тому, якщо розподіл ймовірностей набору даних можна представити великою, дуже розрідженою глибокою нейронною мережею, тоді оптимальну топологію мережі можна побудувати шар за шаром шляхом аналізу кореляційної статистики активацій останнього шару та кластеризації нейронів з великою

кореляцією виходу. Хоча строгий математичний доказ вимагає дуже суворих умов, той факт, що це твердження резонує з добре відомим принципом Гебба [29] – якщо нейрони, які працюють разом, з'єднуються разом – свідчать про те, що основна ідея може застосуватись на практиці навіть за менш суворих умов.

Головними особливостями даної мережі є оптимальна локальна розріджена структура та малі розміри. Оптимальна структура означає, що на карті ознак кожна одиниця може розглядатися як представлення деякої області входу. Тому згорткові ядра можуть закодувати цю єдину область для наступного рівня. Однак є й інші особливості, які складаються з кількох окремих регіонів. Також, паралельно можуть використовуються не тільки згорткові ядра, а також і збільшуючі шари. Усі функції збираються в кінці шару як на рис. 2.2

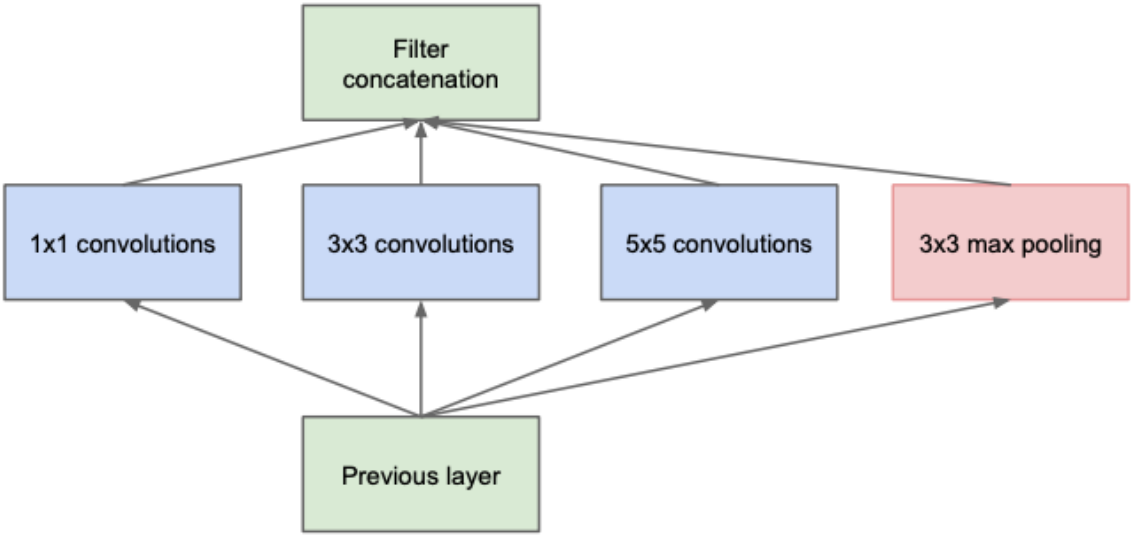


Рисунок 2.2 – Зображення прихованого блоку фунції

Зменшення розмірів досягається шляхом створення локальних структур, введеними раніше, але вартість обчислень все ще дуже висока. Тому автори використовують зменшення розмірності, застосовуючи «1×1» умовні ядро з меншою кількістю фільтрів. Потім карти функцій передаються до більших згорткових ядер, приклад зображено на рис. 2.3.

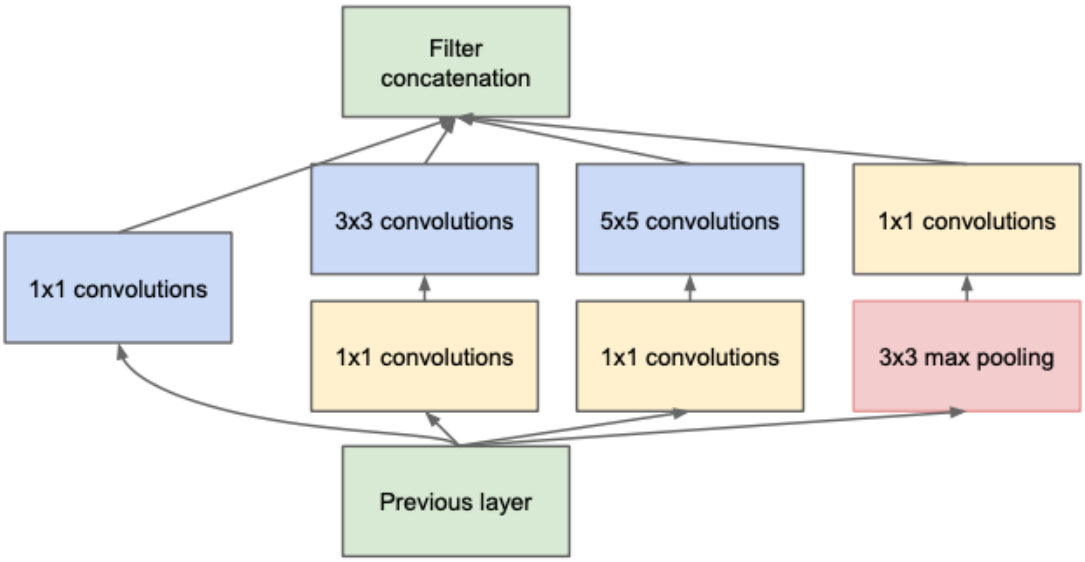


Рисунок 2.3 – Зображення вкладеної мережі зі зменшенням розмірності

Повна структура нейронної мережі InceptionResNet-v1 наведена на рис. 2.4.

type	patch size/ stride	output size	depth	#1×1	#3×3 reduce	#3×3	#5×5 reduce	#5×5	pool proj	params	ops
convolution	7×7/2	112×112×64	1							2.7K	34M
max pool	3×3/2	56×56×64	0								
convolution	3×3/1	56×56×192	2		64	192				112K	360M
max pool	3×3/2	28×28×192	0								
inception (3a)		28×28×256	2	64	96	128	16	32	32	159K	128M
inception (3b)		28×28×480	2	128	128	192	32	96	64	380K	304M
max pool	3×3/2	14×14×480	0								
inception (4a)		14×14×512	2	192	96	208	16	48	64	364K	73M
inception (4b)		14×14×512	2	160	112	224	24	64	64	437K	88M
inception (4c)		14×14×512	2	128	128	256	24	64	64	463K	100M
inception (4d)		14×14×528	2	112	144	288	32	64	64	580K	119M
inception (4e)		14×14×832	2	256	160	320	32	128	128	840K	170M
max pool	3×3/2	7×7×832	0								
inception (5a)		7×7×832	2	256	160	320	32	128	128	1072K	54M
inception (5b)		7×7×1024	2	384	192	384	48	128	128	1388K	71M
avg pool	7×7/1	1×1×1024	0								
dropout (40%)		1×1×1024	0								
linear		1×1×1000	1							1000K	1M
softmax		1×1×1000	0								

Рисунок 2.4 – Схематичне зображення архітектури згорткової нейронної мережі

Нейромережевий підхід з використанням частини кодувальника моделей Variational Autoencoders [30]. Область автокодувальників поділяється на дві моделі: звичайну та генеративну модель автокодувальника. Звичайна модель автокодувальника здатна лише реконструювати свій вхід. Тим часом генеративний автокодер не лише реконструює свій вхід, але й генерує новий

зразок. Обидва вони складаються з мережі кодера та декодера. Однак у деяких типах моделі генеративного автокодера він має дискримінаторну мережу, подібну до генеративної змагальної мережі (GAN) [31]. Прикладом цієї моделі є AAE та WAE.

Деякі подробиці про звичайні автокодери та моделі генеративних автокодерів пояснюються далі.

Звичайний автокодувальник (далі – АК) має цільову функцію, яка полягає в реконструкції вхідних даних у код і назад у вихідні дані з мінімальною можливою помилкою. Звичайна мережа АК складається з двох частин: частини кодувальника, яка стискає вхідні дані мережі в змінні меншої розмірності, який називається кодом; і частина декодувальнинка, яка реконструює приховані змінні назад у свих першочерговий вигляд. Приклад мережі показаний на рис. 2.5. Звичайний АК не призначений для ідеального копіювання своїх вхідних даних, інакше мережа не дізнається жодних значущих представлень. Натомість існує обмеження у звичайній мережі АК, воно розташоване в розмірності латентних змінних і має меншу розмірність, ніж вхідна. Це змушує кодувальника навчатися видобувати деякі важливі функції та зв’язки з вхідних даних, а декодувальник в свою чергу намагається навчитися використовувати ці функції для реконструкції на виході.

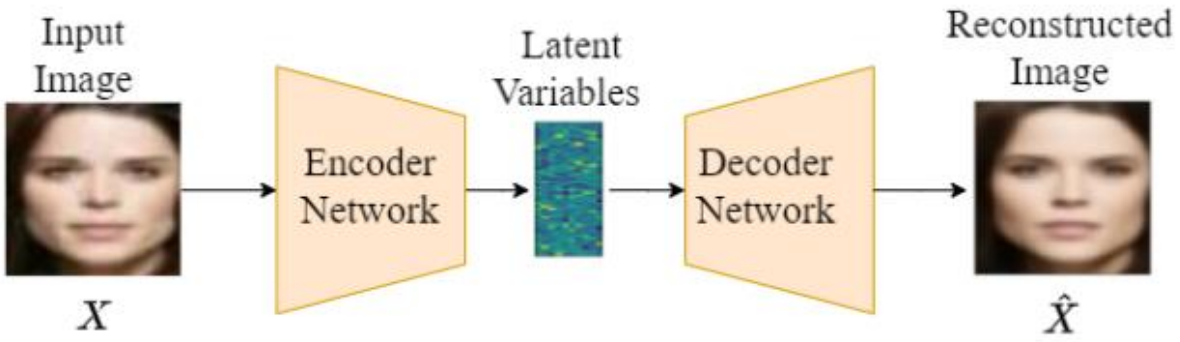


Рисунок 2.5 – Схема роботи звичайного автокудовальника

Варіаційний автокодувальник (далі – ВАК) – це генеративна модель автокодувальника, яка має на меті дізнатися розподіл ймовірностей вхідних даних за навчальними даними [32]. Це дозволяє ВАК створювати нові

правдоподібні варіації вхідних даних на основі зразків із розподілу. Мережа ВАК показана на рис. 2.6.

Ідея ВАК полягає у вибірці прихованих змінних з простору, щоб вони, з відповідною ймовірністю створювали варіації вхідних даних [33]. Розподіл для вибору може бути будь якого типу, однак більшість ВАК використовують стандартний розподіл Гауса, оскільки його легко обчислити.

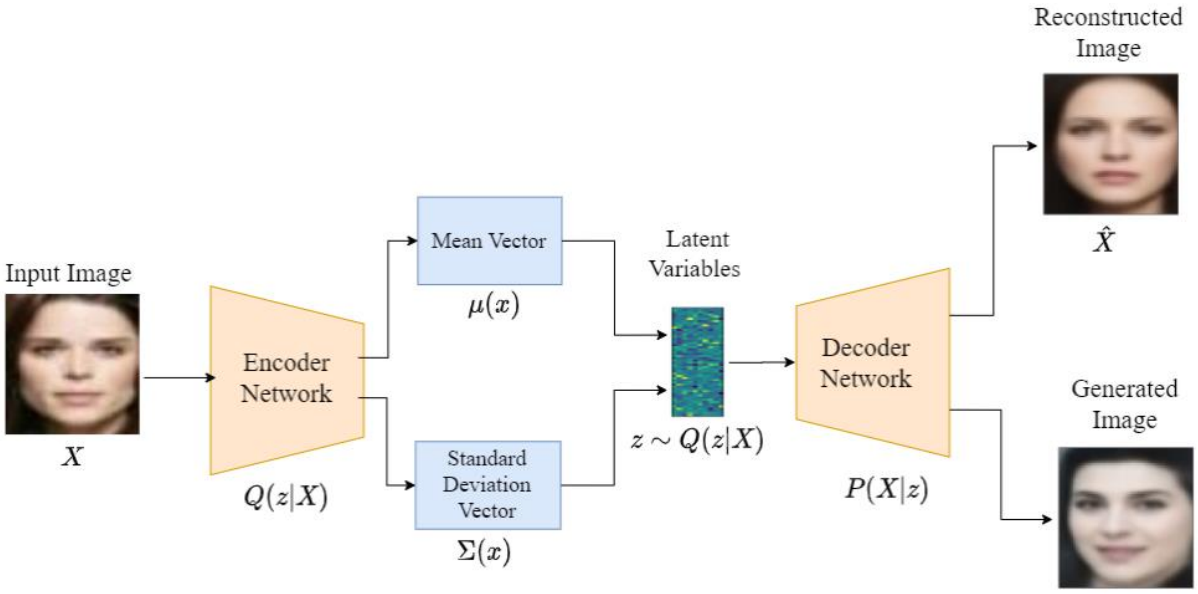


Рисунок 2.6 – Схема роботи варіаційного автокудовальника

Автокодувальники надають можливість автоматичного вивчення функцій з немаркованих даних, що дозволяє проводити неконтрольоване навчання та намагатись виявити загальні характеристики даних, які вивчають наближену функцію ідентифікації шляхом вивчення важливих прихованих характеристик. АК виконують «стиснення» даних до коду, що є важливим кроком для зменшення розмірів та є своєрідним механізмом екстракції різних характеристик з зображення обличчя. Тому даний код можна спробувати використати в якості ідентифікуючого вектора унікальних характеристик користувача. Загальна архітектура для автокодувальників наведена на рис. 2.7.

Encoder Network

Layer Name	Input Channels	Output Channels	Kernel Size	Stride	Padding	Activation Function
Conv + BN	3	128	4	2	1	ReLU
Conv + BN	128	256	4	2	1	ReLU
Conv + BN	256	512	4	2	1	ReLU
Conv + BN	512	1024	4	2	1	ReLU
Flatten			$1024 \times 4 \times 4$			
Fully Connected	$1024 \times 4 \times 4$	z_{dim}	-	-	-	-

Decoder Network

Layer Name	Input Channels	Output Channels	Kernel Size	Stride	Padding	Activation Function
Fully Connected	z_{dim}	$1024 \times 8 \times 8$	-	-	-	-
Reshape			$1024 \times 8 \times 8$			
ConvTranspose + BN	1024	512	4	2	1	ReLU
ConvTranspose + BN	512	256	4	2	1	ReLU
ConvTranspose + BN	256	128	4	2	1	ReLU
ConvTranspose + BN	128	3	1	1	0	-

Рисунок 2.7 – Схематичне зображення архітектури мережі автокодувальника

Нейромережевий підхід для детекції та побудови графу унікальних вузлових точок користувача. У сукупності можна зробити висновок, що НМ є прихованим виконавцем, роботу якого важко розшифрувати. Те, що люди помітно відрізняються зовнішністю, особливо рисами обличчя, очевидно. Так, наприклад, навіть близнюки відрізняються положенням очей і їх найменшими рисами. Тому не дивно, що перше історично адресоване автоматичне розпізнавання осіб на основі зображень обличчя ґрунтувалося на відборі та порівнянні певних антропометричних ознак осіб. Цей підхід давно використовується в практичній криміналістиці, але вимірювання та порівняння проводяться вручну.

Суть методу полягає в обліку статистичних зв'язків між розташуванням антропометричних точок. На наявній вибірці зображень осіб, знятих в анфас. На зображенні відображення розмітка розташування антропометричних точок. На кожному зображенні точки пронумеровані в однаковому порядку. Дані були анотовані з використанням розмітки 68 орієнтирів (на зображенні червоні, так і зелені орієнтири). Між очна відстань, використовується для нормалізації положення голови, вона визначається між зовнішніми точками очей.

Анотації є частиною 68-точкового набору даних iBUG 300-W [34], на якому відбувалось тренування предиктора орієнтирів обличчя. Приклад анотації зображено на рис 2.8.

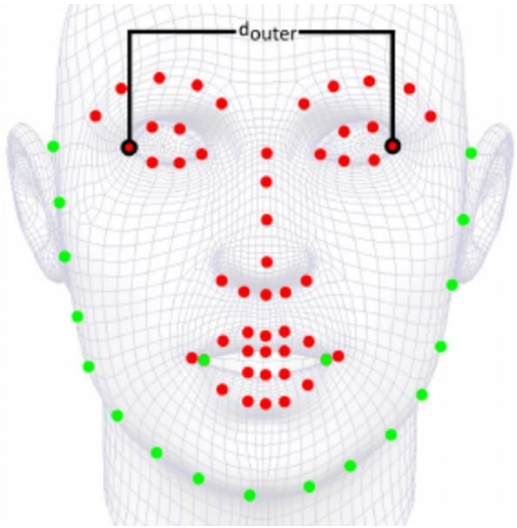


Рисунок 2.8 – Розмітка зображення обличчя з 68 точок

Щоб привести координати на всіх зображеннях в одну систему, так званий узагальнений прокрустів аналіз, результатом якого є приведення всіх точок в один масштаб і центрування. Далі обчисліть середнє значення форми та коваріаційну матрицю для всього набору зображень. Відповідно до коваріаційної матриці обчислюються власні вектори, а потім упорядковуються в порядку спадання відповідно до їхніх відповідних власних значень. Моделі ASM визначаються матрицями та векторами середньої форми. Позиціонування моделі ASM на нових зображеннях, що не входять до навчальних зразків, здійснюється в процесі вирішення задачі.

Архітектура детектора ознак обличчя використовує ResNet-50 [35] як «хребет» моделі, та поєднується з чотирма модифікованими модулями «Hourglass» [36] і одним кроком підвищення дискретизації для створення карт балів для кожної орієнтирної точки обличчя вхідного обличчя. Архітектура моделі зображена на рис 2.9.

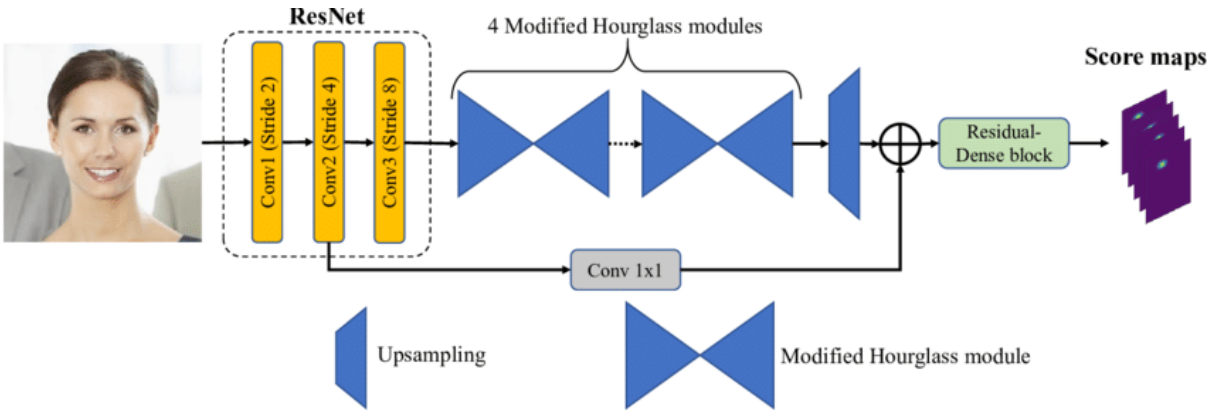


Рисунок 2.9 – Архітектура детектора ознак обличчя ResNet-50

Оптимізації, але основною метою AAM і ASM є не розпізнавання облич, а точне позиціонування облич і тіл людей на зображення Виміряйте точки для подальшої обробки. Майже в усіх алгоритмах необхідним кроком для зміщення класифікації є вирівнювання, що означає вирівнювання зображень людей за їхнім фронтальним положенням відносно камери або вирівнювання набору облич.

Щоб досягти цього етапу, необхідно розташувати антропометричні точкові особливості всіх осіб на зображенні - зазвичай це центр зіниці або куточок ока. Різні дослідники виділяють різні групи таких точок. Щоб знизити обчислювальні витрати систем реального часу, розробники виділяють не більше 10 таких точок. Моделі AAM і ASM точно розроблені для точної локалізації цих антропометричних точок на зображеннях обличчя.

При використанні цього підходу основна проблема, з якою доводиться стикатися розробникам систем розпізнавання, полягає у виборі набору характеристик, які однозначно описують конкретну людину. При цьому слід також враховувати наступні вимоги: точки на обличчі або риси обличчя, за якими базується розпізнавання, не повинні бути закриті зачісками, бородами, масками тощо; щоб забезпечити незалежність процесу розпізнавання від масштаб зображення, рекомендовано описати точки розпізнавання в системі їх взаємозв'язку; обрана система балів повинна забезпечувати відносну стабільність процесу розпізнавання при незначних змінах ракурсу зйомки

(легкий поворот голови, нахил, зміна виразу обличчя тощо), кількість балів ознаки системи, що задовольняють зазначеним вимогам, має бути найменшою. , оскільки розрахунок алгоритму Вартість зазвичай пропорційна їх кількості. На даний момент існує багато робіт, присвячених дослідженню розпізнавання з використанням різних наборів ознак і аналізу продуктивності систем, побудованих на них.

2.2 Розробка архітектури системи

Перевірка обличчя – це завдання ідентифікації особи за допомогою джерела, як-от зображення, відео чи канал камери її обличчя. Існують різні методи перевірки обличчя, залежно від того, як ми аналізуємо та виділяємо риси та візерунки обличчя із зображення. Це завдання можна розбити на три під задачі:

- детекція обличчя;
- передобробка входу зображення обличчя;
- екстракція унікальних характеристик з фото обличчя;
- класифікація отриманого вектору унікальних характеристик відповідно до найближчого доменного вектору.

Завдання розпізнавання обличчя є частиною практичного застосування теорії розпізнавання образів. Рішення даних задач активно використовується починаючи з сучасних сервісів та закінчуючи військовими задачами.

Людина може впізнавати обличчя інших людей завдяки веретеноподібній звивині — ділянці мозку на межі потиличної та скроневої часток. Ключові особливості, які мозок вирішує розпізнати, це очі, ніс, рот і брови. Крім того, мозок людини відновлює все обличчя, а то й половину, і може розпізнати людину лише по частині обличчя. Мозок усереднює всі обличчя, які він бачить, і шукає відмінності від цієї усередненої версії. Таким чином, людям досить складно відрізняти людей іншої раси [37].

Системи розпізнавання обличчя використовують комп’ютерні алгоритми для вилучення конкретних унікальних деталей обличчя людини. Ці деталі, такі як відстань між очима або форма щелепи, потім перетворюються в математичне зображення та порівнюються з іншими даними обличчя, зібраними в базі даних. Дані про обличчя, які часто називають шаблоном обличчя, відрізняються від фотографії тим, що містять лише певні деталі, за якими можна відрізнити одне обличчя від іншого. Замість позитивного розпізнавання невідомих осіб деякі системи розпізнавання облич призначені для обчислення оцінки ймовірності збігу між невідомою особою та певним малюнком обличчя, що зберігається в базі даних. Замість того, щоб просто повертати один результат, ці системи запропонують кілька потенційних збігів, упорядкованих за ймовірністю правильної ідентифікації. Системи розпізнавання обличчя відрізняються за здатністю ідентифікувати людей за таких складних умов, як погане освітлення, низька якість зображення та неоптимальний кут огляду.

Як було вказано вище, однією з перших задач, яку необхідно вирішити для побудови моделі ідентифікації користувача за обличчям – це безпосередньо є процес детекції обличчя користувача.

Детекція обличчя передбачає встановлення обмежувальної рамки, яка містить обличчя на даному зображенні. В ідеалі обмежувальний прямокутник має повністю охоплювати обличчя, не обрізаючи важливі форми та риси обличчя та не включаючи більше, ніж необхідно для подальшої ідентифікації користувача. Наприклад, включення заднього фону чи обличчя інших людей може завадити класифікатору правильно провести класифікаційний процес.

Для проведення процесу детекції було обрано багатозадачну каскадну згортову мережу MTCNN [38].

MTCNN – це каскадна мережа з трьох ЗНМ, які є своєрідними етапами в процесі детекції обличчя.

Перший етап має повністю підключену мережу пропозицій (Fully Connected Proposal Network, P-Net), яка використовується для отримання вікон-кандидатів і зменшення перекриття та кількості ящиків. На даному етапі

відбувається прийом вхідних даних як піраміди зображень, що складається з копій вхідного зображення в різному масштабі. Це надає моделі широкий діапазон розмірів вікон на вибір і допомагає моделі бути незмінною в масштабі. Архітектура нейронної мережі P-Net зображена на рис. 2.10.

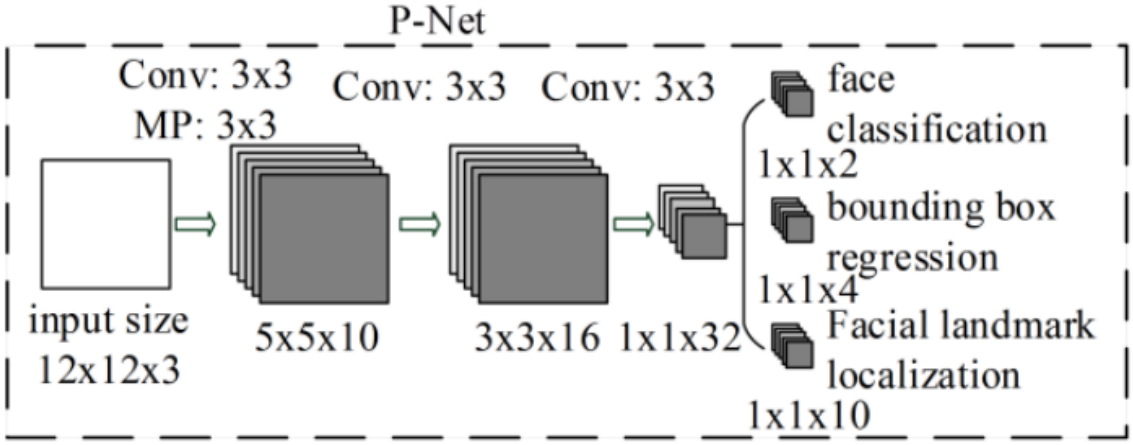


Рисунок 2.10 – Архітектура нейронної мережі P-Net

Другий етап — Згорткова уточнююча мережа (Refine Network, R-Net). На даному етапі відбувається додаткове зменшення кількості блоків і об’єднання різних кандидатів, які перекривають одне одного за допомогою технології «non-maximum suppression» (NMS) [39]. Архітектура нейронної мережі R-Net зображена на рис. 2.11.

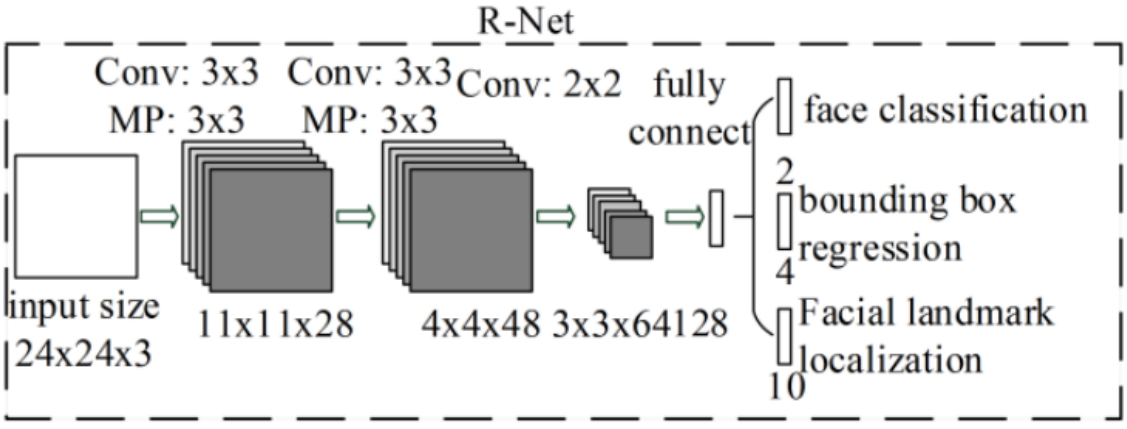


Рисунок 2.11 – Архітектура нейронної мережі R-Net

Вихідна мережа (Output Network, O-Net) на третьому етапі виконує тіж самі дії, що й R-Net, але в більшій кількості і додає 5-точковий орієнтир очей, носа та рота в остаточну рамку, що містить виявлене обличчя. Архітектура нейронної мережі O-Net зображена на рис. 2.12

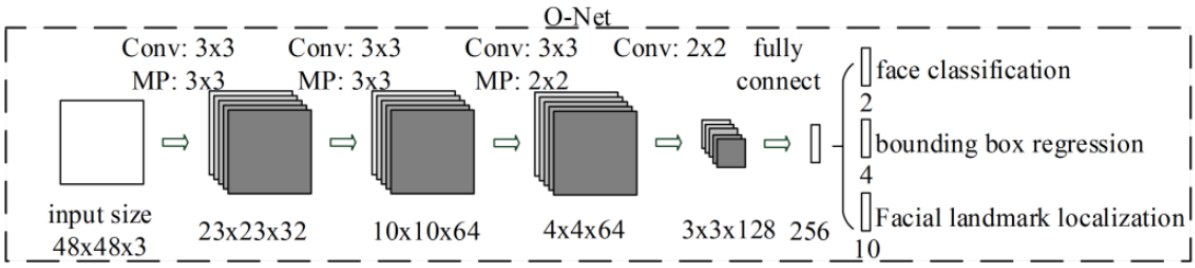


Рисунок 2.12 – Архітектура нейронної мережі O-Net

Результатом роботи детектора є 5 фіксуючих точок та встановлена обмежувальна рамка на обличчі користувача. Приклад роботи з вказанням усіх проміжних етапів детектора MTCNN зображено на рис. 2.13

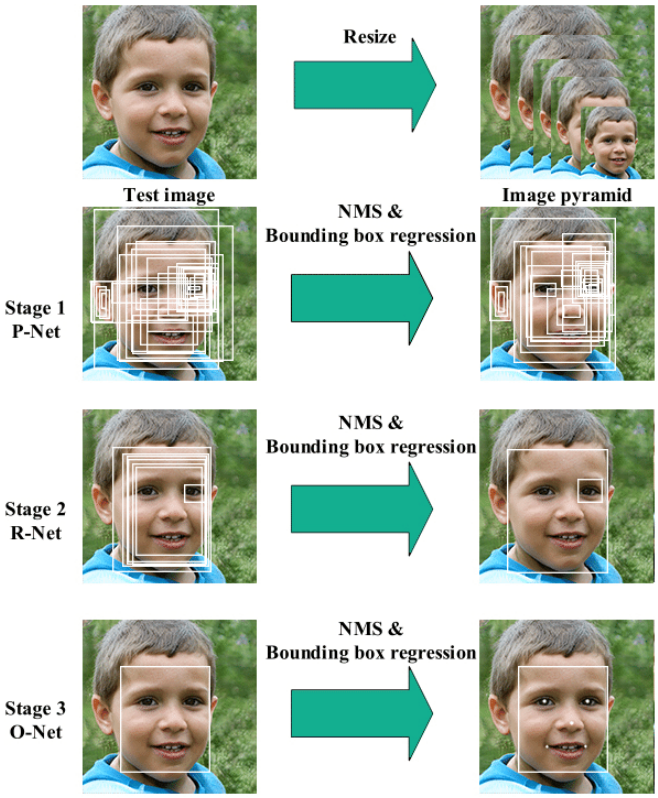


Рисунок 2.13 – Приклад роботи детектора MTCNN

Посилаючись на формальну постановку задачі необхідно приведення всіх обличчя до одного розміру, це відбувається шляхом стандартизації фотографій обличчя за ключовими точками.

Для цього необхідно застосувати алгоритм перетворення. Спочатку необхідно виявити наявні апріорні положення ключових точок в одиничному квадраті, далі знаючи обраний розмір зображення, розраховуються координати ключових точок на зображенні шляхом масштабування. За необхідності

відбувається виділення ключових точок наступного обличчя. Для кожного з облич побудувати афінне перетворення, що переводить набір точок, після проведення перетворення необхідно зробити обрізку зображення. Схема даного процесу зображена на рис. 2.14.

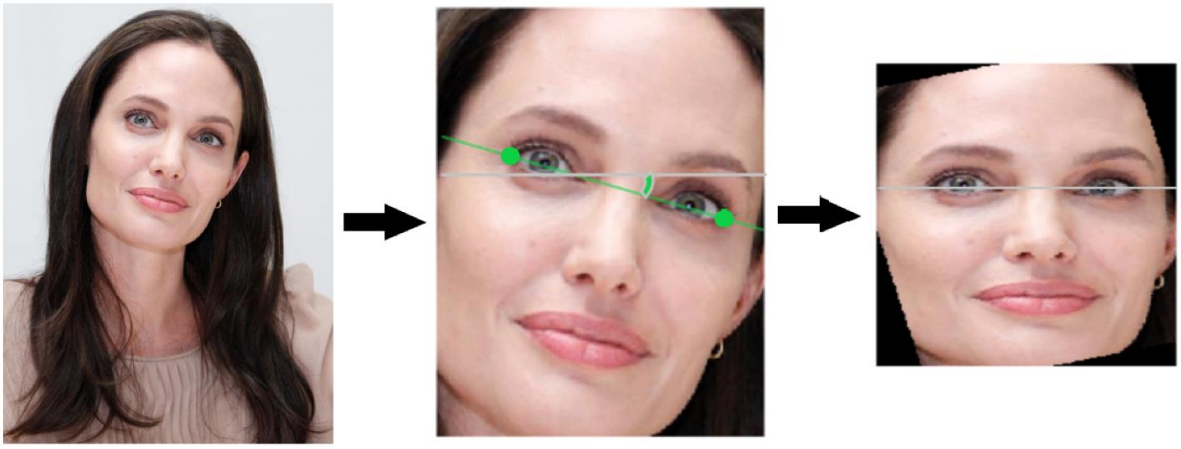


Рисунок 2.14 – Схема перетворення вхідного зображення

Фінальним кроком процесу процесу передобробки є стандартизація зображення, шляхом підрахунку стандартизації зображення розмістивши розподіл значень вхідної матриці в діапазоні середнього та стандартного відхилення по базі навчання.

Для нейромережевого підходу і автокодувальник процес передобробки завершується на цьому етапи. Але для нейромережевого підхіду для детекції та побудови графу унікальних вузлових точок користувача використовується додаткова модель для екстракції з отриманих точок саме векторного представлення унікальних характеристик користувача, які вже можна порівнювати між собою та встановлювати приналежність.

Програмне забезпечення для розпізнавання облич базується на можливості спочатку розпізнавати обличчя, що саме по собі є технічним рішенням. На обличчі є певні помітні орієнтири. Це вершини та долини, які утворюють різні риси обличчя. На обличчі людини близько 80 вузлів. В основному програмним забезпеченням робиться фокус саме на: відстані між очима, ширині носа, глибині очної ямки, вилицях та на лінії щелепи і підборіддя. Різні вузлові існують на

кожному обличчі - верхівці підборіддя, зовнішньому краю кожного ока, внутрішньому краю кожної брови тощо, як показано на рис 2.15.

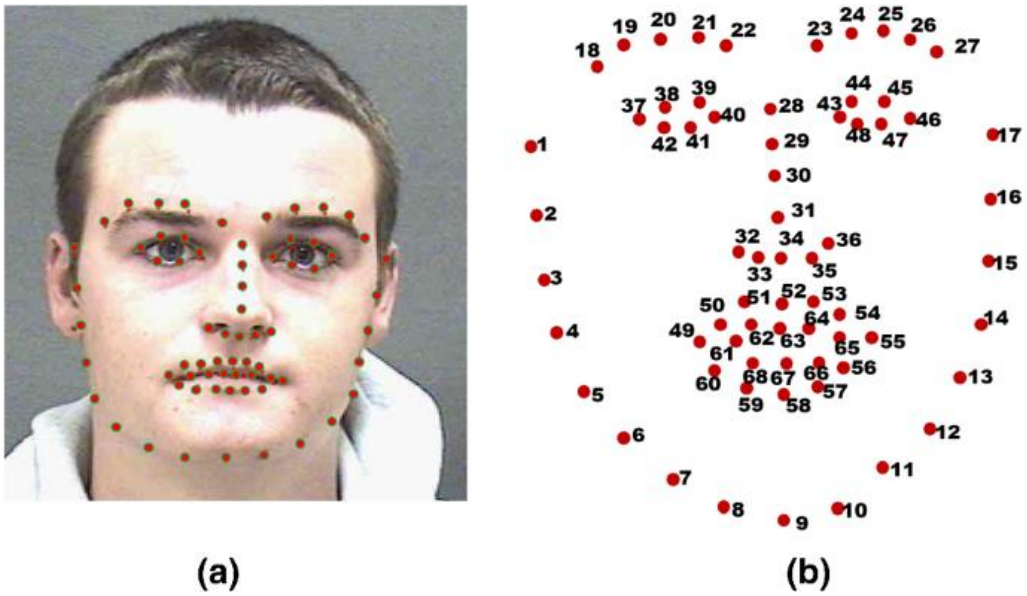


Рисунок 2.15 – Визначення орієнтирів обличчя. Частина a – орієнтири обличчя. Частина b – положення та порядок 68 точок на обличчі

Як і було вказано в минулому підрозділі, алгоритми машинного навчання здатні знаходити такі вузлові точки на будь-якому обличчі. Але просто отримати дані точки недостатньо для того щоб ідентифікувати за ними користувача. Для порівняння даного набору вузлових параметрів необхідний спеціальний алгоритм за допомогою якого ми зможемо визначати наскільки той чи інший набір точок схожий, чи відмінний один від одного. Якраз для встановлення такої відповідності та створення відповідних векторів характеристик використовується наступна модель ResNet-34 [40].

Дана мережа була навчена на наборі даних з 3 мільйонів облич. Цей набір даних отримано з кількох наборів даних [41]. Навчання мережі проводилось з випадково ініціалізованих ваг та з використання структурованої метричної втрату, яка намагається спроектувати всі ідентичності в неперекриваючі кулі з певним радіусом.

На вхід дана мереже приймає як вхідне зображення обличчя, так і попередньо визначені орієнтири. Виходом мережі є вектор розміром 128. Архітектура мережі зображена на рис. 2.16.

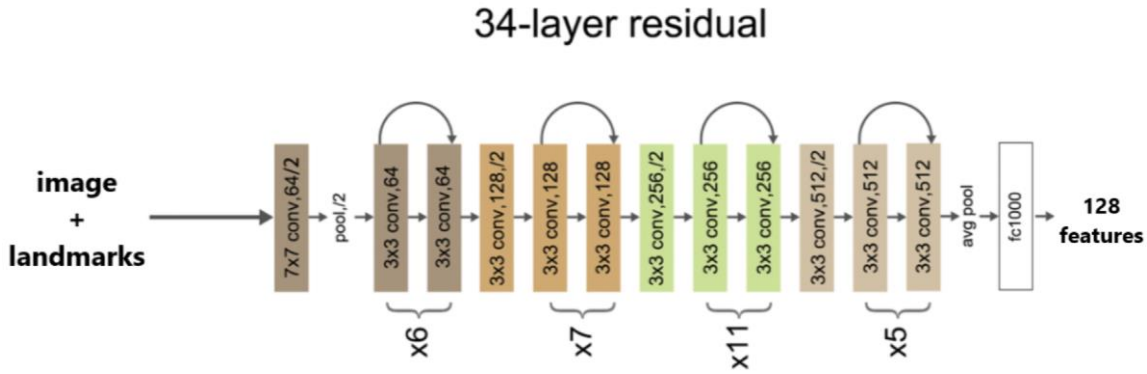


Рисунок 2.16 – Архітектура мережі ResNet-34

Після процесу передобробки необхідно перейти до побудови структури моделі ідентифікації користувача за допомогою обличчя

2.3 Побудова структури моделі ідентифікації обличчя користувача

Після виконання розпізнавання обличчя та обробки введення користувачем матриці обличчя необхідно перейти до етапу, безпосередньо пов’язаного із завданням розпізнавання обличчя. Для того, щоб розрізнити обличчя, нам потрібно знайти особливості в кожній людині. Перше питання, яке постає перед нами, — як організувати розпізнавання. Найпростіший спосіб розпізнати обличчя — порівняти невідоме обличчя, отримане на другому кроці, з усіма обличчями в нашій базі даних. Тому під час кожного процесу розпізнавання ми звертаємося до бази даних. На перший погляд ідея оптимальна, однак, якщо обсяг даних великий, то це збільшить час дискретизації, більш того, варто розглянути варіант перенесення цих даних у хмару. Якщо ми говоримо про дуже великі обсяги даних, це може спричинити проблеми із затримкою між запитом і відповіддю на сервер. А як зазначено [42], для більшості проектів із розпізнавання, швидкість розпізнавання є на першому місці. Тому такий спосіб розпізнавання не може бути використаний.

Через неефективність і високу обчислювальну складність попередніх методів пропонується метод виділення кількох основних рис обличчя. У цьому випадку виникає проблема вибору цих ознак. На перший погляд розмір або колір очей, довжина носа, розмір губ, форма брів можуть здатися основними ознаками,

за якими людина впізнає обличчя. Однак, як показано в дослідженні [43], ці функції не є цінними для комп’ютерного розпізнавання обличчя. Ця проблема пов’язана з тим, що комп’ютер не може оцінити загальне людське обличчя за допомогою звичайного алгоритмічного підходу, оскільки він оцінює зображення піксель за пікселем.

Для вирішення задачі ідентифікації користувача за допомогою обличчя пропонується використовувати 3 глибинних нейронних мережі (deep neural network, DNN), які навчені для визначення унікальних числових характеристик обличчя. А саме: нейромережевий підхід з порівнянням вихідних векторів характеристик моделі повертає вектор унікальних характеристик розміром 512, нейромережевий підхід з використанням кодуючої частини моделей Variational Auroencoders повертають вектор розміром 64 та нейромережевий підхід для детекції та побудови графу унікальних вузлових точок користувача повертає вектор унікальних характеристик розміром 128.

Процес отримання унікального вектора характеристик з такої нейронної мережі працює за таким принципом:

1) Завантажити зображення особи до детектора та отримати виокремлене зображення обличчя.
2) Провести передобробку отриманого зображення.
3) Передати отриману матрицю до нейромережевих моделей.
4) Виходом з моделей і буде 3 відповідних унікальних вектори характеристик користувача по фото обличчя.
5) Зберегти отримані вектори до бази для використання в якості основного класифікованого вектору для порівняння..

Схема вище описаного процесу відображена на рис 2.17.

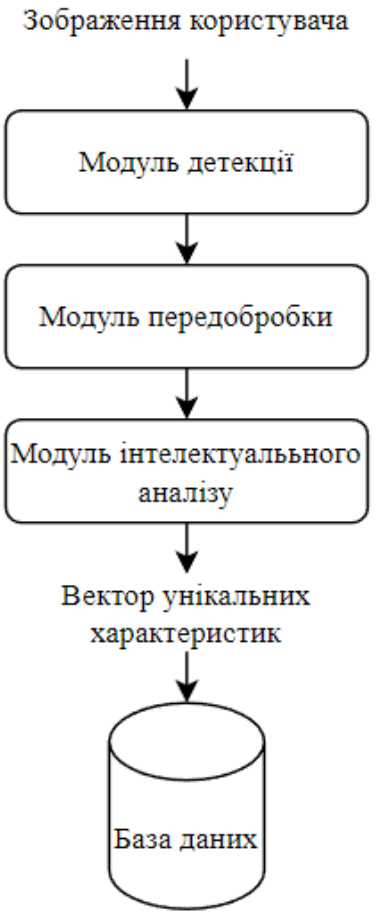


Рисунок 2.17 – Загальний вигляд процесу отримання унікального вектора характеристик

Для того щоб провести перевірку зображень користувача в процесі роботи необхідно виконати наступний ряд дій:

1) Завантажити зображення користувача, що підлягає перевірці.
2) Провести передобробку отриманого зображення.
3) Передати отриману матрицю до нейромережевих моделей та отримати відповідні вектори унікальних характеристик по зображенню обличчя.
4) Підвантажуємо з бази основні вектори для порівняння.
5) Перевіряємо по певному порогу, чи є в базі вектори з достатньо близькою відстанню. Якщо є – користувачу, що перевіряється, ставиться відповідна мітка, яка належить тому користувачу, який виявився найближчим до нього. Якщо ж ні – користувачу ставиться мітка, про те що він є невідомою особою.

Схема вище описаного процесу перевірки зображень користувача в процесі роботи відображена на рис 2.18.

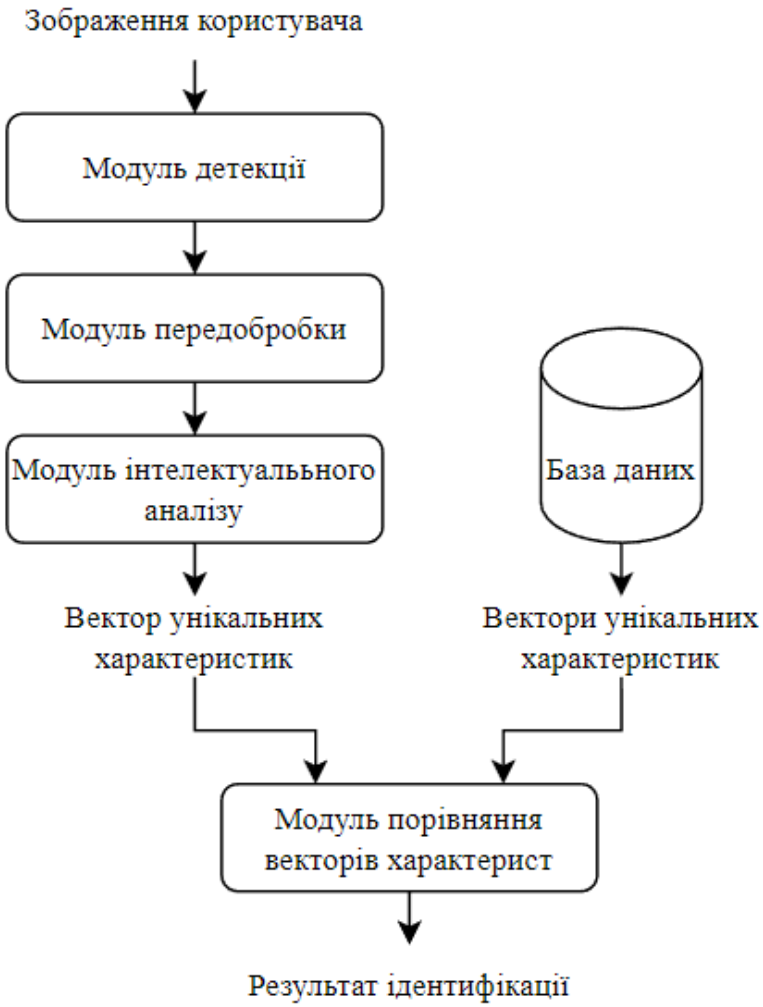


Рисунок 2.18 – Загальна схема проведення перевірки зображень користувача в процесі роботи

Використання глибинної нейронної мережі для генерації унікальних числових характеристик обличчя користувача є процесом досить складним, який вимагає великої бази даних облич і значної обчислювальної здатності комп’ютера. Навіть із графічною картою NVidia Telsa, оскільки модель навчається на графічній карті NVidia з підтримкою CUDA, яка підтримує вищі 24 різні швидкості, процес навчання займає близько 24 годин. Тому найкращим рішенням є використання попередньо навченої глибокої нейронної мережі.

Останній крок алгоритму полягає в порівнянні вже наявних даних, а саме векторів унікальних ознак конкретного обличчя, отриманих з моделей нейронної мережі.

Цей етап можна реалізувати за допомогою бази даних - як було сказано вище, обсяг даних великий, що може істотно знизити продуктивність програми. Однак цей спосіб організації можна використовувати для невеликих обсягів даних, коли перед нами стоїть завдання розпізнати невелику групу людей, або коли недостатньо фотографій для якісного навчання методів опорних векторів. Для порівняння векторів характеристик будуть використовуватись 3 методи: Евклідова відстань, Cosine similarity та Manhattan Distance. Було обрано ці 3 метрики для перевірки продуктивності та точності моделей в залежності від різних метрик, які застосовуються для визначення відстані між векторами.

Після того як були сформовані структури моделі, маємо можливість сформувати загальну схему ідентифікації користувача за обличчям. Дана схема представлена на рис. 2.19.

Як видно з рисунку 2.19, 3 моделі ізольовані одна від одної, на вхід до них подаються оброблені вхідні дані. Далі кожний вихідний вектор перевіряється з списком вихідних векторів зареєстрованих користувачів. При ідентифікації користувача за обличчям, можливо виділити декілька випадків роботи:

– в випадку, якщо одна з моделей в момент спрацювання іншої моделі не приймала ніяких дій, її голос не буде врахований;

– в випадку, якщо спрацювали усі моделі, сигналізатор візьме як результат, різницю між векторами з найбільшою відстанню. Це потрібно для того, щоб вберегти систему від хибних спрацювань.

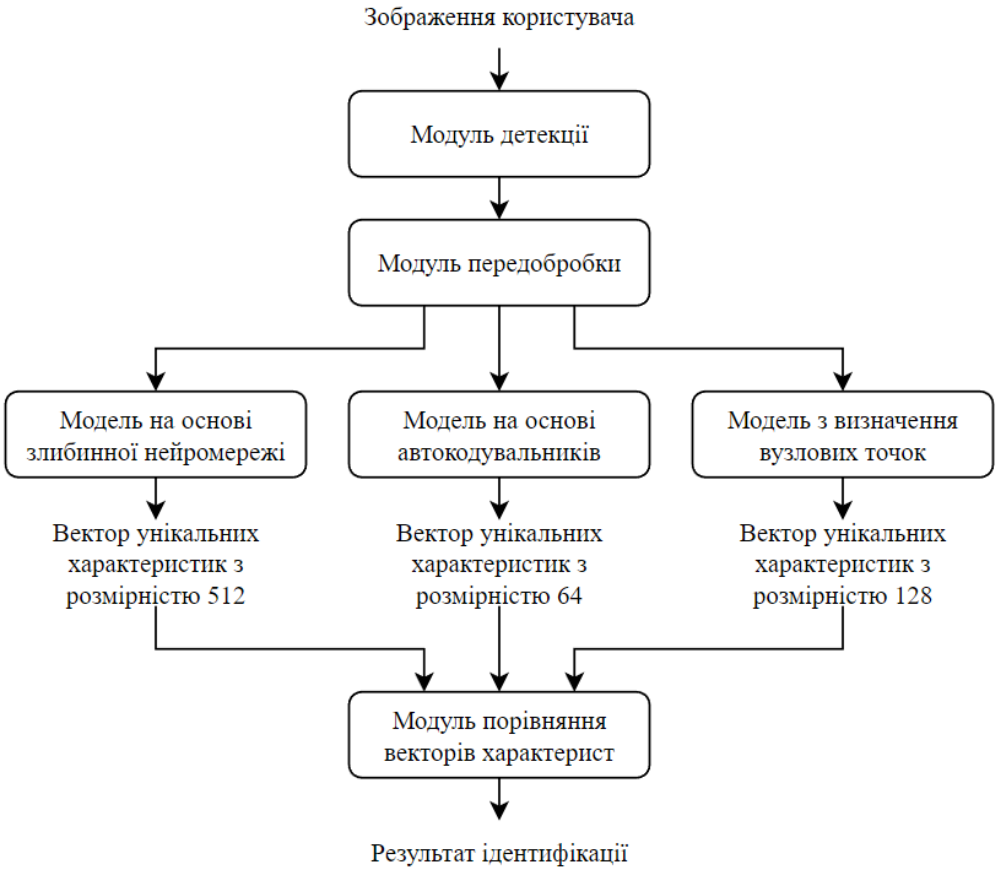


Рисунок 2.19 – Загальна структура моделі ідентифікації користувача за допомогою обличчя

Отже, було розроблено систему ідентифікації користувача за периферійними пристроями. Розроблено структуру моделі ідентифікації користувача за обличчям. Проаналізовано та розроблено вигляд подання вхідних даних до моделі. Було вибрано найбільш оптимальні методи та моделі, які вибрані з врахуванням поставленої задачі та цілі даної роботи. Розроблена повна функціональна схема роботи програмного засобу, яка буде використовуватись для розробки програмного додатку та слугуватиме орієнтиром в процесі його тестування.

3 РЕАЛІЗАЦІЯ ТА АНАЛІЗ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧА

3.1 Програмна реалізація модуля ідентифікації користувача за обличчям

Даний алгоритм точно показує принцип за яким працюють біометричні системи розпізнавання по обличчю – робиться серія знімків обраної людини за допомогою відеокамери, зображення спеціальним чином обробляється та передається до моделей, щоб провести аналіз.

Дана програма біометричної ідентифікації користувача за обличчям людини була розроблена на мові програмування Python, в середовищі розробки Visual Studio Code.

Для вирішення деяких завдань в процесі розробки були використані наступні сторонні бібліотеки:

- Dlib [44];
- OpenCV [45];
- Pytorch [46];
- Tensorflow [47].

Переваги і недоліки відкритої бібліотеки DLIB

Dlib – це міжплатформна бібліотека програмного забезпечення загального призначення з відкритим кодом, написана мовою програмування C++. Дизайн значною мірою вплинули ідеї проектування за контрактом і розробка програмного забезпечення на основі компонентів. Це означає, що перш за все, набір незалежних програмних компонентів, кожен з яких супроводжується великою документацією та режимами ретельного налагодження. Dlib є біблиіотекою з відкритим віхідним кодом, що дозволяє безкоштовно використовувати його в будь-яких розробках.

OpenCV (Open Source Computer Vision Library) – це бібліотека з відкритим вихідним кодом, яка дуже корисна для програм комп’ютерного бачення, таких як аналіз відео, аналіз записів із камер відеоспостереження та аналіз зображень.

OpenCV написано на C++ і містить понад 2500 оптимізованих алгоритмів. Коли ми створюємо програми для комп'ютерного зору, які ми не хочемо створювати з нуля, ми можемо використовувати цю бібліотеку, щоб почати зосереджуватися на проблемах реального світу. Сьогодні багато компаній використовують цю бібліотеку, наприклад Google, Amazon, Microsoft і Toyota. Багато дослідників і розробників роблять свій внесок. Ми можемо легко встановити його в будь-яку ОС, наприклад Windows, Ubuntu і MacOS. OpenCV є створеною для задач з високою ефективністю обчислювання з фокусом на розробці задач в режимі реального часу.

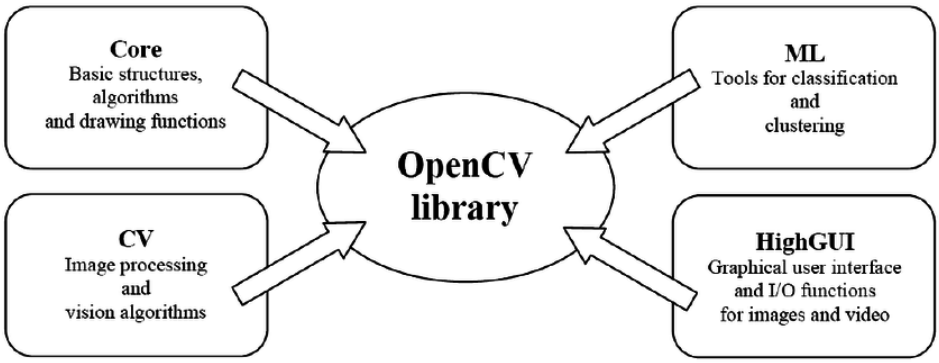


Рисунок 3.1 – Компоненти бібліотеки OpenCV

Вся система ідентифікації поділена на три модулі обробки: модуль ідентифікації по зображенню обличчя, модуль зберігання даних і інтерпретації результатів. Взаємодія користувача з програмою організовано через графічний інтерфейс. Структура програми відображена на рис. 3.2.

Рисунок 3.2 – Зв’язки модулів програми

Розроблені моделі ідентифікації, являються основою модуля ідентифікації, що ведуть даний процес на наданих даних у вигляді векторів. Даний модуль також включає в себе алгоритми попередньої обробки вхідного зображення:

Видача характеристик відбувається кожен раз, як додається нове зображення користувача до бази. По завершенню навчання, отримані вектори характеристик користувача записуються на жорсткий диск і вивантажується з оперативної пам’яті.

На вхід до моделей ідентифікації подається матриця зображення на перевірку, що має формат який ідентичний розмірності навчальній вибірці. Відбувається визначення вектора, що найближче розташований до даного тестового вектору. За допомогою тестування різних підході до розразунку відстані були отримані результати, які надають свідчення, що Евклідова відстань дає кращу якість виділення ідентифікованого зображення серед всієї вибірки в порівнянні з іншими відстанями.

Емпірично на основі проведених експериментів було вибрано порогове значення відстані в 4.6.

На виході є індекс знайденого зображення в навчальній матриці і відстань до нього від тестового вектора.

Модуль попередньої обробки дає змогу готувати зображення для їх подальшої обробки. Так, є методи завантаження зображень у різних форматах. Модуль дозволяє вивести зображення до необхідної для моделі розмірності, з тією умовою, що особи на зображенні розташовані точно по центру.

Модуль зберігання даних і інтерпретації результатів відповідає за зберігання навчальних даних для кожної людини, організовує взаємодію між графічним інтерфейсом і модулями ідентифікації, інтерпретує і об’єднує результати ідентифікації по обом факторам.

При додаванні нової людини в вибірку відбувається отримання вхідних даних від графічного інтерфейсу: дані отримані з веб-камери та ім’я нового користувача. Дані передаються в модулі ідентифікації, де з них виділяються вектора особливостей, які зберігаються в пам’ять. Для подальшої роботи самі файли, не потрібні, задля економії системних ресурсів. Кожна людина представляється набором векторів зображень його особи, векторами унікальних характеристик і одним зображенням його особи, яке не використовується для ідентифікації і слугує лише для наочного відображення результату ідентифікації.

Для ідентифікації проводиться аналогічна завантаження зображення і даних голосу. Завантажується матриця навчальної вибірки зображень і разом з вектором для перевірки передається в модуль ідентифікації по зображенню, де і відбувається ідентифікація.

Використовується векторно-центроїдний підхід, те враховується голос з усіх кластерів. На виході модуля ідентифікації є дані про індекс і видаленні найбільш близького вектора зображення.

Зобразимо дану схему як діаграму послідовності. Діаграма послідовності показує як передається фокус керування від одного модуля системи до іншого (рис. 3.3)

Рисунок 3.3 –Діаграма послідовності

Діаграма пакетів показує зв’язок між певними пакетами системи та визначає як вони взаємодіють між собою (рис.3.4). Користувач безпосередньо працює з пакетом який містить в собі модулі графічного інтерфейсу. Цей пакет взаємодіє з усіма іншими передаючи їм дані. Конектор забезпечує з’єднання з сервером на якому розташована база даних.

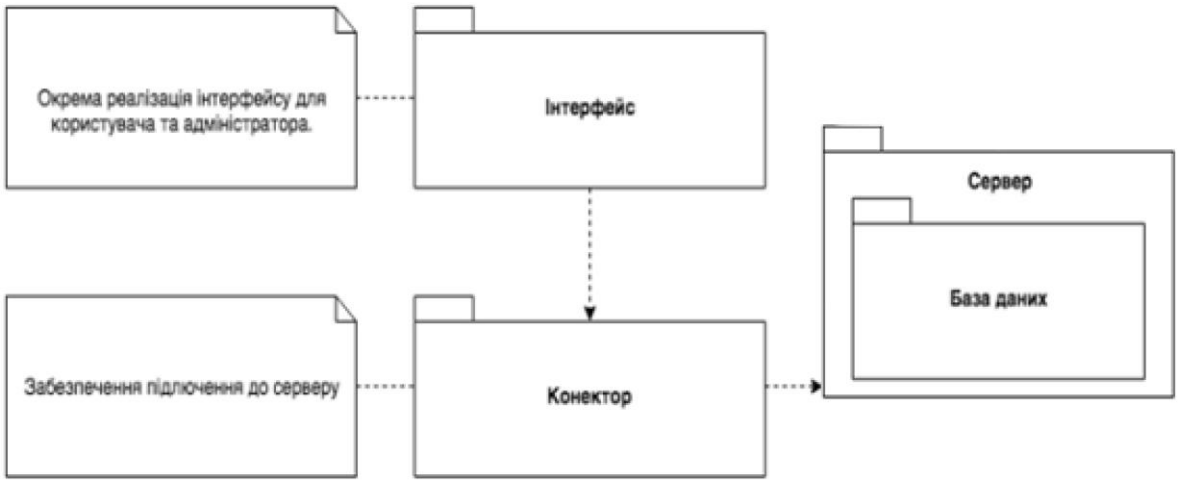


Рисунок 3.4 – Діаграма пакетів

3.2 Оцінка ефективності біометричної системи ідентифікації

Дуже часто на рівні кінцевого користувача потрібна детальна оцінка ефективності впровадження та використання біометричних систем у конкретних умовах конкретних моделей та розташування відеокамер, освітлення приміщення. Це може бути необхідно як у великомасштабних системах, так і як засіб біометричного контролю використання комп'ютерів, доступних для широкої публіки в домашніх умовах.

Ефективність – є функцією системи, що характеризує її здатність виконувати поставлені перед нею завдання відповідно до поставлених цілей за певних умов, з певною якістю, тобто ступенем пристосованості системи до виконання раніше поставлених завдань. що. Визначення ефективності системи необхідне порівняння різних систем для однієї й тієї ж мети.

Виходячи з вищевикладеного, стосовно біометричних систем, визначення ефективності є здатність системи достовірно встановлювати особу особи, що ідентифікується. Відомо, що це відповідає загальноприйнятому поняттю яке надійність біометричної системи.

Однак, через те, що біометрична система є не демонстративною, а реально використовується користувачами для вирішення реальних завдань, врахування технічних недоліків і одночасно всіх факторів, важливих для кінцевого користувача є не простою задачею. Тому питання, які стосуються практичної сторони, є принциповим, це означає, що замість суто технічної оцінки ефективності системи ще необхідно проаналізувати і загальну ефективність споживачів. Така інтерпретація враховує різні сукупності як технічних і економічних так і емпіричних факторів, причому не лише оптимальність технічних значень, а і загальну ефективність системи шляхом порівняння економічних показників та оцінок користувачів. Для аналізу використовуються загальноприйняті методи.

Розглядаючи прикладну систему більш глибоко, тобто з урахуванням її цільового призначення, необхідно врахувати вплив підсистем, пов'язаних із

біометричними засобами ідентифікації. Такі як, наприклад, надійність системи обмеження фізичного доступу, яка безпосередньо залежить не тільки від надійності біометричного сканера, але і від базової міцності замку, що закривається ним, а комп'ютерні системи контролю доступу відкриті для можливості альтернативної ідентифікації які залежать від участі третіх осіб заснованих виключно на вкрадених паролях. Розгляд ефективності біометричних засобів, що входять до складу прикладної системи у вигляді окремих підсистем чи функціональних елементів виконується далі.

Визначення ефективності має сенс лише конкретного суб’єкта, особливості якого диктуються використовуваними при цьому підходами і методами. В недалекому минулому системи біометричної автентифікації широко використовуються в системах безпеки різних організацій, тому необхідно при тестуванні враховувати різні потреби в залежності від користувача. Дослідження ефективності різних галузях проводяться вже довгий період. Втім, замість теоретично чітко визначеного набору рішень є лише багатий набір різних підходів, точок зору, концепцій тощо.

Як і в будь-якому іншому проекті, існує потреба в порівняльній оцінці ефективності біометрії, щоб остаточно визначити найкращі альтернативи і таким чином зробити вибір на користь найкращого рішення. Оскільки пошук найефективнішого біометричного рішення за своєю суттю є завданням оптимізації, можна використовувати два концептуально різні підходи.

Перший підхід представляє об’єкт дослідження (в даному випадку цільову систему, що реалізує біометрію) як «чорний ящик» без аналізу внутрішніх процесів об’єкта. Він статистично встановлює кореляційні зв’язки між вхідними керуючими об’єктами та вихідними параметрами, які є показниками якості та ефективності. Головною перевагою цього підходу є його загальність і можливість застосування до всіх випадків оптимізації. Однак статистичні дослідження (наприклад, повні факторні експерименти) необхідно проводити за індивідуальними протоколами для кожного конкретного випадку, результати яких стануть непридатними, якщо зміниться властивості досліджуваної системи.

Другий підхід заснований на системному моделюванні і передбачає розробку і використання спеціальних критеріїв оптимальності - характерних показників розв'язків оптимізаційних задач, значення яких оцінюють ступінь їх відповідності заданим вимогам, тобто оптимальним рішенням оптимізаційних задач. При цьому оптимальні результати досягаються варіюванням вхідних параметрів для підтримки оптимальних значень цих критеріїв як мінімального значення критерію або, навпаки, його максимального значення, яке фактично вимірюється опосередковано через управління. Критеріїв оптимальності в задачі може бути багато, а загальної методики їх вибору немає, а вибір ґрунтується в основному на досвіді або на якихось рекомендаціях. Хоча в задачах оптимізації використовуються досить різні величини, існує багато загальних критеріїв, які можна застосовувати майже всюди. Наприклад, за базовими економічними показниками можна оцінити абсолютно будь-яку матеріальну систему, а за обчислювальною складністю як будь-яку алгоритмічну модель.

Оскільки в даному випадку неможливо провести суттєві статистичні дослідження при аналізі біометричних систем, для вибору оптимального рішення буде використано другий підхід. При цьому, через специфіку завдання, параметри системи, які чітко визначають кінцеву якість і ефективність, не розглядаються як критерії оптимізації, а безпосередньо розглядають параметри самої системи. Значення таких характеристичних метрик можна легко змінювати під час рішення без проміжних розрахунків. Таким чином, створення відповідної моделі системи замінюється логічними міркуваннями, суб'єктивними припущеннями та вибором відомих варіантів.

Як було показано вище, загальна споживча ефективність біометричних систем характеризується показниками ефективності – параметрами системи, які є об’єктивно оптимальними критеріями.

Зрозуміло, що загальні показники для характеристики ефективності можна розділити на групи, які об’єднують параметри зі схожим змістом. У конкретних випадках можна виділити наступні групи показників продуктивності системи:

– ефективність, на практиці це технічна ефективність, надійність розпізнавання, що визначається декількома технічними показниками системи;

– надійність розпізнавання, що визначається декількома технічними показниками системи;

– ресурсоємність – це сукупність характеристик, що визначають витрати на впровадження та підтримку системи, тобто її економічну ефективність.

Далі розглянемо ці групи факторів окремо та визначимо показники, що впливають на ефективність системи біометричного розпізнавання за геометричною формою особи, як еталон оптимальності для подальшого порівняння та оцінки ефективності.

Як було показано вище, технічні показники ефективності характеризують надійність біометричної системи, яка описується за допомогою математичної статистики, оскільки метод біометричного контролю має імовірнісний характер, а основою будь-якої біометрії є статистика.

Під час сканування система порівнює дані користувача зі стандартами та дає відповідь «збігів немає». З математичної точки зору процес автентифікації — це перевірка статистичної гіпотези, в якій можливі два типи помилкових висновків: відхилення гіпотези, яка насправді є істинною, помилкова заборона доступу законному користувачеві, «помилкові спрацьовування, і якщо гіпотеза неправильна , потім прийняти припущення, помилково пропустити аутсайдера та промахнутися. Ці події називаються «Помилка першого роду» і «Помилка другого роду» відповідно. Імовірність цих біометричних помилок представлена коефіцієнтами FAR (False Accept Rate) і FRR (False Rejection Rate) [48]. Зазвичай передбачається нормальний розподіл ймовірностей. Значення FAR і FRR можуть бути виражені як безрозмірними коефіцієнтами (0,00-1,00), так і у відсотках. Значення FAR фактично описує ймовірність біометричного збігу двох людей, а також може опосередковано робити висновки про схильність системи до «злому». Значення FRR визначає мінімальну якість і кількість даних, які надає система для правильної ідентифікації особи.

Оскільки сьогодні не можна гарантувати повну безпомилковість жодної системи, ймовірність хибнопозитивних і хибнонегативних ідентифікацій має найбільше практичне значення для оцінки якості біометричної системи. Теоретично, чим краще система, тим менше значення FRR і FAR. Однак у більшості випадків важливо одне зі значень. Зокрема, для логічних або фізичних систем контролю доступу першочерговим завданням є запобігання доступу неавторизованого персоналу. Очевидно, що для цього потрібен дуже низький FRR, навіть за рахунок FAR.

Імовірність помилки (FRR і FAR) значною мірою залежить від особистості суб'єкта автентифікації та може бути визначена для кожного окремо, хоча, очевидно, однієї людини недостатньо, щоб зробити висновок про надійність усього біометричного рішення. У цьому контексті за аналогією також згадуються «помилки третього типу», коли розпізнавання неможливе через відсутність або серйозне пошкодження окремих ознак, які використовуються в алгоритмі. Імовірність цієї помилки - FER (Failure to Enrollment Rate) - показує відсоток людей, які не змогли завершити свою реєстрацію в системі. Такі невдачі можуть бути пов'язані з недостатньою підготовкою, середовищем, ергономічними умовами, які роблять біометричний фактор просто непридатним для деяких людей. не можна забути. Помилки I і II роду в принципі невиправні, мова може йти лише про зниження їх ймовірності до практично допустимих значень. Оскільки статистика похибок визначається методом і тривалістю випробування, кількістю і характером статистичних вибірок, ймовірність похибки є функцією не тільки надійності методу, але й багатьох умов експлуатації. Часто алгоритм характеризується якоюсь «ідеальною» основою або просто для гарної підгонки, де нечіткі та розмиті кадри відкидаються. Сканери також можуть значно впливати на кінцеву статистику FAR і FRR. У практичних ситуаціях ці цифри можуть відрізнятися в десять разів.

На практиці ймовірність помилок типу 1 і типу 2 у біометричних системах автентифікації може бути набагато вищою, і, незважаючи на спроби зменшити їх, вони значно відрізняються від реалізації до реалізації. Тому для спрощення

використання сучасні біометричні рішення мають налаштування чутливості, які дозволяють вибрати найкраще співвідношення точності розпізнавання та зручності використання для кожної ситуації. У той же час система використовує настроювані пороги ймовірності, щоб визначити, наскільки точно дані користувача відповідають існуючим тестам реєстрації. Фактично, змінюючи чутливість, ви можете встановити значення FAR і FRR.

Для системи розпізнавання контурів обличчя значення FAR становить 0,1%, а FRR – кілька відсотків, що досить посередньо для сучасної системи безпеки. Для деяких алгоритмів заявлений FRR = 0,1% є аналогічним FAR, але отримана ними основа навряд чи є репрезентативною (вирізаний фон, той самий вираз обличчя, та сама зачіска, освітлення).

Видно, що статистичні показники методу досить скромні і їх необхідно враховувати на практиці. Отже, щодо системи аутентифікації для контролю доступу до об’єктів із середнім рівнем безпеки слід зазначити наступне. Необхідно встановити максимальну чутливість алгоритму зниження FRR 71, трохи зменшити її з часом у разі занадто частих помилкових відмов у доступі, або організувати перевірку стандартних умов: розташування камер, навчання співробітників. , хороше регулювання освітлення Зона. У невеликій організації з 30 або менше співробітників цілком прийнятна для системи ідентифікації очікувати одну або дві помилки відмови в доступі на день.

Швидкість роботи системи залежить від часу, який система витрачає на ідентифікацію користувача. Чим критичнішим стає цей час, тим більшу кількість ідентифікаційних процедур необхідно виконати протягом певного періоду часу. Наприклад, 5 секунд – це невелика кількість для одноразового тесту, але якщо сотні людей проходять його щодня, багато разів на день, сукупна втрата часу буде величезною. Однак якість біометричної системи визначається не тільки швидкістю розвитку технологій. Також важливими є емпіричні показники, які характеризують суб’єктивну оцінку системи користувачами та визначають швидкість роботи системи на основі простоти її використання. Розглянемо найбільш очевидні і важливі з цих показників.

Зручність використання системи відображає, наскільки складно користуватися біометричним сканером і чи можна його ідентифікувати «на ходу». Головним чином він вирішує, чи достатньо правильно обрана система щодо соціальних характеристик об'єкта. Приклад: в офісному контролі доступу можуть бути черги в зоні аутентифікації на початку робочого дня, і якщо співробітники йдуть на роботу в один і той же час, то складність аутентифікації висока. Розпізнавання осіб особливо зручно тим, що немає фізичного контакту та ідентифікації людини без його участі за допомогою зовнішньої камери виявлення, що можливо лише за умови зйомки невеликої кількості об’єктів у базі та невеликого потоку людей. Сумісність з існуючими системами — це можливість інтегрувати біометричні засоби в існуючу інфраструктуру. Розглядаючи конкретну систему контролю доступу до комп'ютера, необхідно переконатися, що вона працює належним чином з наявним апаратним і програмним забезпеченням, і проаналізувати її потенціал для інтеграції встановлені системи захисту. Конфлікти в роботі підсистем неминуче позначаються на загальній продуктивності.

Кількісна оцінка таких показників у задачах оптимізації виконується за умовною безрозмірною шкалою де кожній альтернативі присвоюється її оцінка в одиницях балів. Найвища оцінка явно повинна відповідати найкращому значенню показника. Для кількісної оцінки однотипних численних характеристик і властивостей можна використовувати метод експертної оцінки. Експертна оцінка – це процедура отримання будь-якої оцінки для подальшого прийняття рішень на основі висновку експерта. Експертна оцінка особливо важлива при вирішенні завдань, які неможливо розв’язати звичайними аналітичними методами, наприклад, вибір найкращого рішення серед наявних варіантів рішення, прогнозування розвитку процесу, пошук розв’язку складних проблем.

Ефективність методу і правильність прийнятих рішень безпосередньо визначаються експертним відбором експертної групи. Порівняно з кількістю респондентів у загальному опитуванні кількість учасників панелі значно менша.

При цьому інформація, отримана в експертних опитуваннях, як правило, дуже достовірна і достовірна, оскільки респонденти є висококваліфікованими фахівцями в даній галузі. Для порівняльного аналізу ефективності біометричних систем необхідно скласти максимально повний перелік варіантів вирішення проблем, за якими можна визначити зазначені вище показники.

3.3 Дослідження та тестування отриманої системи ідентифікації користувача

Оскільки, метою даної роботи є дослідження та вдосконалення ефективності методів розпізнавання та ідентифікації осіб – весь набір зображень був створений під дану мету.

Було підібрано 10 осіб: 5 які були зареєстровані до системи, тобто для однієї з фотографій було створено вектори унікальних характеристик, а 5 не були зареєстровані. Для кожного з даних користувачів було зібрано набір даних розміром близько 100 зображень. Загальний вигляд набору даних для дослідження наведено в таблиці.

Після проведення цих процедур були сформовані набори для обробки за допомогою досліджуваних методів розпізнавання, в таблиці 3.1 показано, як розподілилися за вибірками зображення, залежно від того, скільки частин ділився вихідний набір зображень.

Нейромережевий підхід з порівнянням вихідних векторів характеристик моделі є однією з основних моделей в даній системі. Виходом даної моделі ідентифікації слугує вектор розмірністю 512, сам по собі вектор не говорить про свою приналежність до одного з користувачів, які зареєстровані чи не зареєстровані в системі. Тому для забезпечення даної особливості необхідно використовувати спеціальні алгоритми для визначення відстані між різними векторами. Дані алгоритми можуть забезпечувати класифікацію вихідного вектора моделі відповідно до одного з існуючих векторів, які відносяться до попередньо зареєстрованого користувача.

Таблиця 3.1 – Об'єм тестового набору при розбитті вихідного набору зображень класу на різну кількість частин

Номер користувача	Кількість зображень
Зареєстровані користувачі	
1	97
2	100
3	95
4	98
5	99
Не зареєстровані користувачі	
1	99
2	97
3	95
4	99
5	100

З кожним зображенням вказаних користувачів буде відбуватись екстракція векторів унікальних характеристик та порівняння їх з наявними зареєстрованими векторами в базі. Порівняння буде проводитись по вказаним метрикам, а по отриманим значенням буде розраховуватись середнє значення точності розпізнавання зареєстрованих та не зареєстрованих користувачів. Результат роботи моделі глибинної нейронної мережі наведено в таблиці 3.2.

Для попередньої оцінки результатів ідентифікації буде відображено результати роботи програми при ідентифікації різних користувачів з допомогою зображення їх точкових векторів у простора, де кожен із них позначений відповідно своїм кольором. Кількість точок кожного користувача на рисунку, залежить від розміру вхідних даних, яка була отримана від нього, тобто чим більше вхідних даних, тим більше зрозумілішим і чіткішим буде результат користувача на діаграмі.

Таблиця 3.2 – Результат роботи моделі на основі глибинної нейронної мережі

Номер користувача	Точність, %		
	Метрика відстані		
	Euclidean	Cosine	Manhattan
Зареєстровані користувачі			
1	97	99	96
2	100	100	99
3	95	99	87
4	98	99	100
5	99	99	99
Не зареєстровані користувачі			
1	99	97	89
2	97	98	99
3	95	99	97
4	99	96	94
5	100	98	96

Для відображення векторів характеристик використовується t-SNE [49] є найпопулярнішим методом візуалізації даних секвенування. Метою t-SNE є створення дво- чи тривимірного вбудовування набору даних, який існує в багатьох вимірах, щоб вбудовування можна було використовувати для візуалізації. Під вбудовуванням мається на увазі проектування даних із великих розмірів на вектори в меншому просторі. Вбудовування відбувається шляхом мінімізації різниці між околицями (тобто відстанями від комірки до набору близьких комірок) у вихідному високовимірному просторі та нижньому вимірному просторі вбудовування. t-SNE — це оптимізаційна задача, де алгоритм ітеративно вивчає серію перетворень, щоб кожне наступне перетворення краще мінімізувало цю різницю між високою та низькою розмірністю відстаней сусідства.

Цей підхід зберігає локальну структуру даних. Тобто вектори, які розташовані близько у високовимірному просторі (тобто мають невеликі

евклідові відстані), також будуть близькі в низьковимірному просторі. Однак це також означає, що глобальна структура не буде збережена. Це означає, що відстань між «кластерами» на графіку не має жодного значення Даний алгоритм має гіперпараметри, це параметри, визначені користувачем, які визначають результат алгоритму.

Скупчення даних одного і той самого кольору означає, що програма може успішно ідентифікувати користувачів та розташовує його дані разом із його іншими даними, що в свою чергу підтверджує успішність ідентифікації. Проте, на рисунку також є моменти коли точки одного кольору, накладаються на точки іншого кольору, це може бути пов’язано як із алгоритмами перетворення і виниканням від цього певного побічного ефекту так із тим, що риси обличчя різних користувачів дійсно можуть бути в чомусь схожі. У разі накладання усіх точок різного кольору в одному і той самому місці, це могло б свідчити про неправильну роботу програми та дуже незначний процент достовірності правильної ідентифікації користувача. Приклад даного розподілу зображено на рис. 3.5.

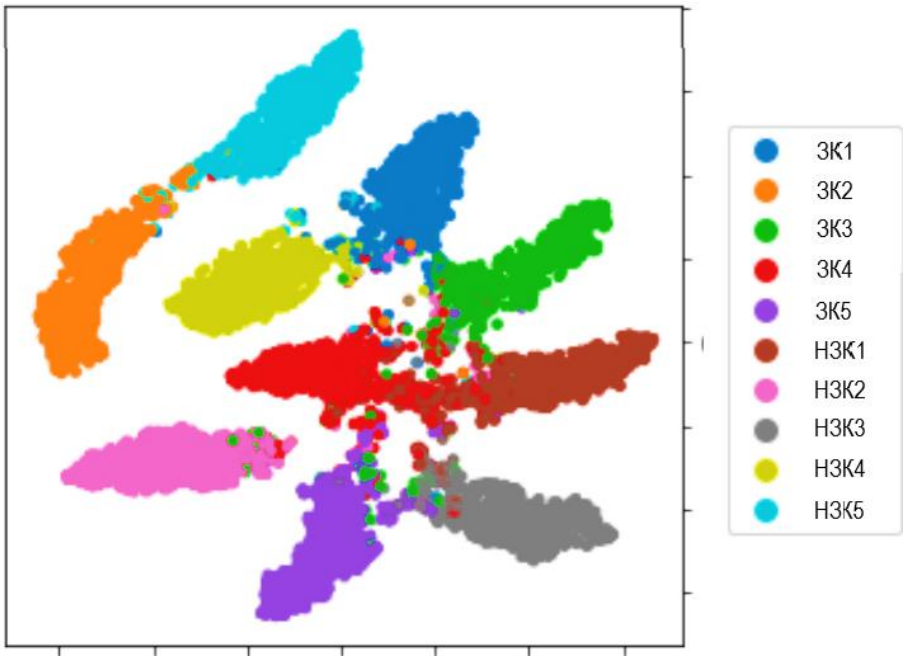


Рисунок 3.5 – Діаграма вихідного вектору у 2-х вимірному форматі

Для Евклідової метрики відстані були розраховані показники FAR та FRR. Дані показники показуються на скільки модель пов’язана на значення

встановленого порогу для визначення близькості векторів. Дані показники зображені на рис. 3.6.

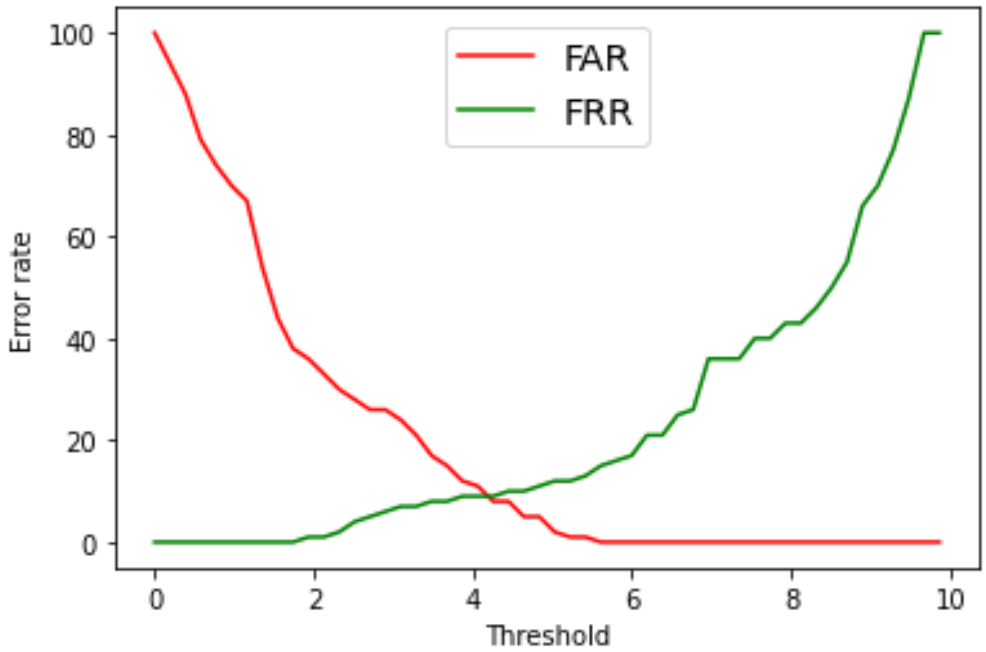


Рисунок 3.6 – Показники FAR та FRR

Нейромережевий підхід з використанням кодуючої частини моделей Variational Auroencoders. Виходом даної моделі ідентифікації відводиться вектор розмірністю 64. Тому для забезпечення даної особливості необхідно використовувати спеціальні алгоритми для визначення відстані між різними векторами. Як і з попередньою моделлю тут з кожним зображенням вказаних користувачів буде відбуватись екстракція векторів унікальних характеристик та порівняння їх з наявними зареєстрованими векторами в базі. Порівняння буде проводитись по вказаним метрикам, а по отриманим значенням буде розраховуватись середнє значення точності розпізнавання зареєстрованих та не зареєстрованих користувачів. Результат роботи нейромережевого підходу з використанням кодуючої частини наведено в таблиці 3.3.

Таблиця 3.3 – Результат роботи нейромережевого підходу з використанням кодуючої частини

Номер користувача	Точність, %		
	Метрика відстані		
	Euclidean	Cosine	Manhattan
Зареєстровані користувачі			
1	77	75	71
2	81	82	73
3	76	70	66
4	77	75	69
5	79	77	72
Не зареєстровані користувачі			
1	72	65	69
2	77	75	74
3	72	73	66
4	74	64	69
5	71	70	65

Для оцінки результатів ідентифікації буде відображено результати роботи програми при ідентифікації різних користувачів з допомогою зображення їх точкових векторів у простора, де кожен із них позначений відповідно своїм кольором. В даному прикладі наявне також скупчення даних одних і тих же користувачів.

Скупчення даних одного і той самого кольору означає, що програма може успішно ідентифікувати користувачів та розташовує його дані разом із його іншими даними, що в свою чергу підтверджує успішність ідентифікації. Для даної технології помітно різницю в точності в порівнянні з іншими підходами до ідентифікації. Модель видає список з унікальних характеристик, але самі по собі характеристики не є унікальними і є певними блоками для побудови лиця і тому подібне. Тому візуальна інтерпретація виглядає дещо змішаною. Результат відображено на рис. 3.7.

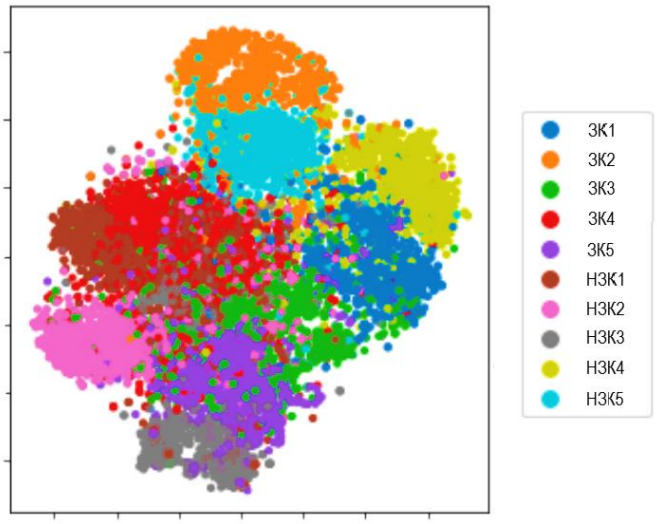


Рисунок 3.7 – Діаграма вихідного вектору у 2-х вимірному форматі

Також в цьому прикладі для Евклідової метрики відстані були розраховані показники FAR та FRR. Дані показники показуються на скільки модель пов’язана на значення встановленого порогу для визначення близькості векторів. Дані показники зображені на рис. 3.8.

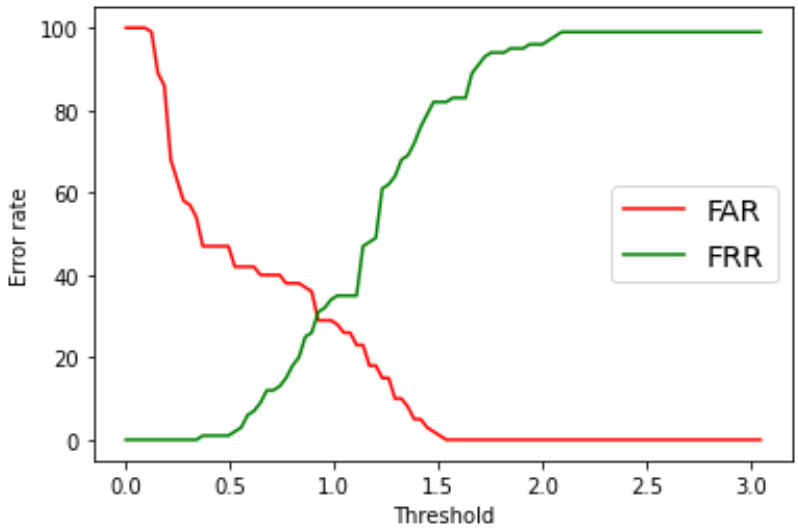


Рисунок 3.8 – Показники FAR та FRR

Нейромережевий підхід для детекції та побудови графу унікальних вузлових точок користувача. Виходом даної моделі ідентифікації відводиться вектор розмірністю 128. Як і з попередніми моделями тут з кожним зображенням вказаних користувачів буде відбуватись екстракція векторів унікальних характеристик та порівняння їх з наявними зареєстрованими векторами в базі. Порівняння буде проводитись по вказаним метрикам, а по отриманим значенням

буде розраховуватись середнє значення точності розпізнавання зареєстрованих та не зареєстрованих користувачів. Результат роботи нейромережевого підходу для детекції та побудови графу унікальних вузлових точок користувача наведено в таблиці 3.4.

Таблиця 3.4 – Результат роботи нейромережевого підходу з використанням кодуючої частини

Номер користувача	Точність, %		
	Метрика відстані		
	Euclidean	Cosine	Manhattan
Зареєстровані користувачі			
1	100	99	100
2	100	100	99
3	95	99	94
4	100	100	100
5	100	100	99
Не зареєстровані користувачі			
1	100	100	100
2	100	100	99
3	100	99	97
4	99	96	100
5	100	98	96

Для оцінки результатів ідентифікації буде відображено результати роботи програми при ідентифікації різних користувачів з допомогою зображення їх точкових векторів у простора, де кожен із них позначений відповідно своїм кольором. В даному прикладі наявне також скупчення даних одних і тих же користувачів. Скупчення даних одного і той самого кольору означає, що програма може успішно ідентифікувати користувачів та розташовує його дані разом із його іншими даними, що в свою чергу підтверджує успішність ідентифікації. Як видно з рисунка, ідея поєднання подачі до моделі точок обличчя та самої фотографії є досить гарною задумкою. Це дозволяє моделі

одразу зрозуміти на що звертати увагу необхідно в першу чергу, та виходячи з цього будувати ваги в процесі навчання. Результат відображено на рис. 3.9.

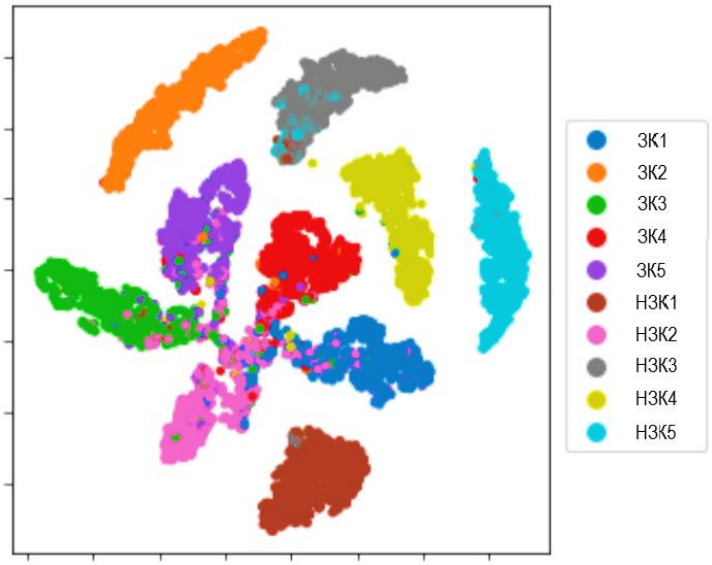


Рисунок 3.9 – Діаграма вихідного вектору у 2-х вимірному форматі

Також в цьому прикладі для Евклідової метрики відстані були розраховані показники FAR та FRR. Дані показники показуються на скільки модель пов’язана на значення встановленого порогу для визначення близькості векторів. Дані показники зображені на рис. 3.10.

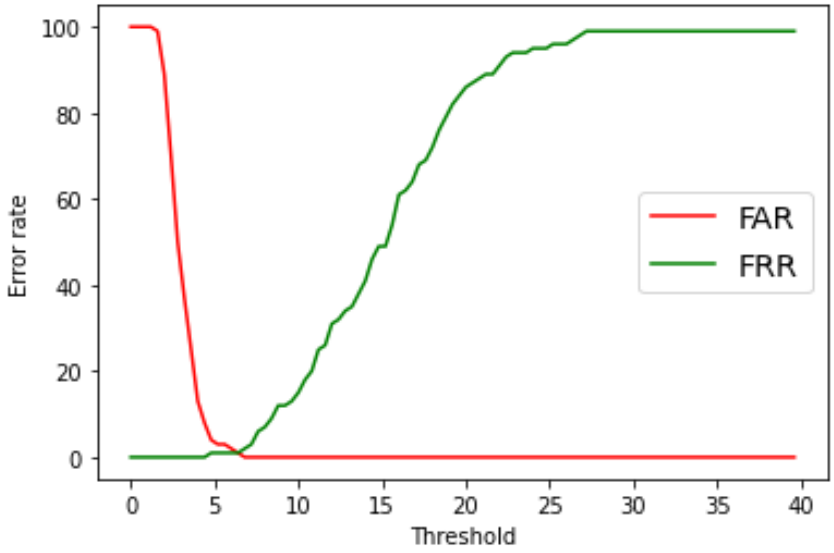


Рисунок 3.10 – Показники FAR та FRR

Отже, за результатами розроблених моделей можна зробити висновок, що розроблені моделі та методи для ідентифікації обличчя користувача є ефективними. Далі необхідно визначити доцільність вище наведеної розробки за допомогою економічних розрахунків.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота з розробки та дослідження «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

1) Проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу.
2) Розраховано витрати на здійснення науково-технічної розробки.
3) Розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів

комп'ютерних систем. Частина 2. Модуль ідентифікації.» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [50].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в	Технічні та споживчі влас-тивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в	Технічні та споживчі властивості продукту значно кращі, ніж в
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					

8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	4	4	5
2. Ринкові переваги (наявність аналогів)	2	3	2
3. Ринкові переваги (ціна продукту)	2	2	3
4. Ринкові переваги (технічні властивості)	1	2	2
5. Ринкові переваги (експлуатаційні витрати)	2	2	2
6. Ринкові перспективи (розмір ринку)	3	4	3
7. Ринкові перспективи (конкуренція)	3	2	3
8. Практична здійсненність (наявність фахівців)	5	5	5
9. Практична здійсненність (наявність фінансів)	3	4	3
10. Практична здійсненність (необхідність нових матеріалів)	4	5	5
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	4	3	4
Сума балів	37	40	41
Середньоарифметична сума балів $СБ_c$	39,3		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [50].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» становить 39,3 бала,

що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

Розробка характеризується такими показниками як:

- унікальність;
- точність;
- швидкість;
- не статичність (ідентифікація за обличчям в реальному часі);
- висока інтерпретованість результатів;
- зручність.

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою [51]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i , \qquad (4.1)$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховуємо за такими формулами:

для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ні}}{I_{аі}}, \tag{4.2}$$

де $I_{ні}$ та $I_{на}$ – чисельні значення конкретного *і*-го технічного показника якості відповідно для нової розробки та аналогу;

для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{аі}}{I_{ні}}; \tag{4.3}$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до таблиці 4.4.

Таблиця 4.4 – Порівняння основних параметрів розробки та аналога.

Показники (параметри)	Одиниця вимірю-вання	Аналог	Проектований пристрій	Відношення параметрів нової розробки до аналога	Питома вага показника
Надійність системи	%	84	92	1,09	0,25
Швидкість ідентифікації об'єкта	с	0,8	0,3	2,67	0,15
Універсальність системи	бал	6,1	8,5	1,39	0,1
Точність ідентифікації об'єкта	%	78	85	1,09	0,3
Зручність інтерфейсу користувача	бал	5	8	1,6	0,2

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 1{,}09 \cdot 0{,}25 + 2{,}67 \cdot 0{,}15 + 1{,}39 \cdot 0{,}1 + 1{,}09 \cdot 0{,}3 + 1{,}6 \cdot 0{,}2 = 1{,}46.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,46 рази.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [50]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.4)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 18200{,}00 \cdot 30 / 21 = 26000{,}00 \ грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
1. Керівник проекту	18200,00	866,67	30	26000,00
2. Ст. науковий співробітник проблем програмного забезпечення	18000,00	857,14	15	12857,14
3. Інженер-програміст	17500,00	833,33	28	23333,33
4. Аналітик систем обробки графічних даних	18000,00	857,14	8	6857,14
5. Консультант-аналітик обробки цифрових зображень	17500,00	833,33	6	5000,00
6. Технік	7530,00	358,57	18	6454,29
Всього				80501,90

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (4.5)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{М_М \cdot К_i \cdot К_с}{Т_р \cdot t_{зм}} , \qquad (4.6)$$

де $М_М$ – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

$К_і$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [50];

$К_с$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$Т_р$ – середнє число робочих днів в місяці, приблизно $Т_р$ = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$С_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 72{,}38$ *грн.*

$З_{р1} = 72{,}38 \cdot 8{,}00 = 579{,}07$ *грн.*

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
1. Встановлення допоміжного обладнання	8,00	2	1,10	72,38	579,07
2. Інсталяція програмного забезпечення	6,00	3	1,35	88,83	533,01
3. Встановлення цифрових обчислювальних систем	3,00	5	1,70	111,87	335,60
4. Відлагодження інтерполяційних модулів системи розпізнавання і ідентифікації	1,50	4	1,50	98,71	148,06
5. Підготовка цифрової експериментальної моделі ідентифікації	8,00	4	1,50	98,71	789,64
6. Формування бази даних підсистеми розпізнавання	12,00	2	1,10	72,38	868,61
7. Формування бази даних для підсистеми ідентифікації	10,00	2	1,10	72,38	723,84
8. Узгодження параметрів системи комп'ютерної графіки для формування реалістичних зображень	3,50	3	1,35	88,83	310,92
9. Тренування системи	3,50	3	1,35	88,83	310,92
Всього					4599,67

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.7)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 10%.

$З_{дод}$ = (80501,90 + 4599,67) · 10 / 100% = 8510,16 грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.8)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (80501,90 + 4599,67 + 8510,16) · 22 / 100% = 20594,58 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.».

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{в\,j}, \quad (4.9)$$

де $Н_j$ – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 3,0 \cdot 207,00 \cdot 1,1 - 0 \cdot 0 = 683,10$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	207,00	3,0	0	0	683,10
Папір для заміток (А5)	130,00	4,0	0	0	572,00
Начиння канцелярське	200,00	3,0	0	0	660,00
Органайзер офісний	237,00	3,0	0	0	782,10
Картридж для принтера	1052,00	1,0	0	0	1157,20
Диск оптичний (CD-R)	20,00	3,0	0	0	66,00
Диск оптичний (CD-RW)	21,00	1,0	0	0	23,10
FLASH-пам'ять (16 ГБ)	110,00	1,0	0	0	121,00
FLASH-пам'ять (32 ГБ)	175,00	1,0	0	0	192,50
Всього					4257,00

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.10)$$

де $Н_j$ – кількість комплектуючих j-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих j-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*).

$К_в = 1 \cdot 1560,00 \cdot 1,1 = 1716,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.8 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Зовнішній жорсткий диск 2.5" 1TB Seagate (STGD2000200)	1	1560,00	1716,00
Графічний адаптер: - тип відеокарти Дискретна - відеокарта GeForce 3060 - об'єм відеопам'яті 12 ГБ	1	5830,00	6413,00
Кабель для передачі даних USB to COM 1.0m Patron (CAB-PN-USB-COM)	1	354,00	389,40
Всього			8518,40

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.11)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i = *1,10…1,12);*

k – кількість найменувань устаткування.

$B_{спец} = 39870,00 \cdot 1 \cdot 1,1 = 43857,00$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
ПК конфігурації Процесор: - Intel core i5 (3,7 ГГц) 12th gen - кількість ядер: 6 ядер Оперативна пам'ять: - оперативна пам'ять 64 ГБ - тип оперативної пам'яті DDR4	1	39870,00	43857,00
Всього			43857,00

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення. Отримані результати зведемо до таблиці 4.10.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.12)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (K_i = *1,10…1,12);*

k – кількість найменувань програмних засобів.

$B_{прг}$ = *100,00 · 1 · 1,1 = 110,00 грн.*

Таблиця 4.10 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Середовище розробки: - Visual Studio	1	100,00	110,00
Всього			110,00

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.13)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (21560,00 \cdot 2) / (2 \cdot 12) = 1796,67$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
ноутбук Asus, характеристики -- Intel Core i3 / RAM 8 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics	21560,00	2	2	1796,67
Місце оператора спеціалізоване	9400,00	5	2	313,33
Офісна оргтехніка	9650,00	4	2	402,08
Лабораторія досліджень програмного забезпечення	520000,00	25	2	3466,67
Прикладний пакет Microsoft Office 2016	7825,00	2	2	652,08
ОС Windows 10	8120,00	2	2	676,67
Всього				7307,50

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.14)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 6,20 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,05 \cdot 240,0 \cdot 6,20 \cdot 0,95 / 0,97 = 74,40$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.12 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
ноутбук Asus, характеристики -- Intel Core i3 / RAM 8 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics	0,05	240,0	74,40
Місце оператора спеціалізоване	0,12	240,0	178,56
Офісна оргтехніка	0,62	4,3	16,53
ПК конфігурації Процесор: - Intel core i5 (3,7 ГГц) 12th gen - кількість ядер: 6 ядер Оперативна пам'ять: - оперативна пам'ять 64 ГБ - тип оперативної пам'яті DDR4	0,42	200,0	520,80
Всього			790,29

4.3.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» відсутні.

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» відсутні.

4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \qquad (4.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів} = 50\%$.

$I_в$ = (80501,90 + 4599,67) · 50 / 100% = 42550,79 грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та

раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}\ , \qquad (4.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$В_{нзв}$ = (80501,90 + 4599,67) · 100 / 100% = 85101,57 грн.

Витрати на проведення науково-дослідної роботи на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}\ . \qquad (4.17)$$

$В_{заг}$= 80501,90 +4599,67 +8510,16 +20594,58 +4257,00 +8518,40 +43857,00 + 110,00 + 7307,50 +790,29 +0,00 +0,00 +42550,79 +85101,57 = 306698,86 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \qquad (4.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

ЗВ = 306698,86 / 0,95 = 322840,91 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, осіб	550	875	925	750

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 5300 осіб;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 15790,00 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 1047,61 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [50]:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.19)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2022 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =35%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2022 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ =(1047,61·5300,00+16837,61·550)·0,83·0,35·(1-0,18/100%)=3528609,14 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ =(1047,61·5300,00+16837,61·1425)·0,83·0,35·(1-0,18/100%)=7038135,33 грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3$ =(1047,61·5300,00+16837,61·2350)·0,83·0,35·(1-0,18/100%)=10748205,88 грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4$ =(1047,61·5300,00+16837,61·3100)·0,83·0,35·(1-0,18/100%)=13756371,19 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.20)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,24;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$ПП$ =3528609,14/(1+0,24)^1+7038135,33/(1+0,24)^2+10748205,88/(1+0,24)^3+ +13756371,19/(1+0,24)^4=2845652,53+4577351,28+5637297,06+5818581,81=18878 882,69 грн.

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \tag{4.21}$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2,1;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 322840,91 грн.

$PV = k_{інв} \cdot ЗВ$ = 2,1 · 322840,91 = 677965,91 грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{4.22}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 18878882,69 грн;

PV – теперішня вартість початкових інвестицій, 677965,91 грн.

$E_{абс} = ПП - PV$ = 18878882,69 - 677965,91 = 18200916,78 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (4.23)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 18200916,78 грн;

PV – теперішня вартість початкових інвестицій, 677965,91 грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1$ = (1+18200916,78/677965,91)$^{1/4}$= 1,30.

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.24)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d =0,1;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,26.

$\tau_{мін}$ = 0,1+0,26 = 0,36 < 1,30 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у

впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.25}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 1,30 = 0,77 р.

$T_{ок} <$ 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Висновки до розділу.

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.» становить 39,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,46 рази.

Також термін окупності становить 0,77 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.».

ВИСНОВКИ

В даній роботі проведений огляд підходів та методів, які були використані для ідентифікації обличчя користувача. Основна увага приділяється підходам, вживаним для ідентифікації людини по його зображенню шляхом пошуку в спеціалізованих базах векторів унікальних характеристик. Дослідження по ідентифікації обличчя користувачів призвели до створення експериментальних систем розпізнавання, але проблема залишається відкритою. У роботі запропонована загальна схема ідентифікації та розпізнавання людей на основі трьох обраних методів на основі нейронних мереж, а саме: антропометричні точки обличчя людини, глибинна нейронна мережа та кодуюча частина автокодувальної мережі.

Метою роботи було вдосконалення існуючих моделей та методів ідентифікації обличчя користувача на базі нейронних мереж. Дана мета була досягнута шляхом розробки моделей ідентифікації обличчя користувача та програмного застосунку, який дозволяє отримати простий але надійний продукт для захисту програмних систем.

Для вирішення задачі побудови системи ідентифікації обличчя користувача проведено:

- аналіз методів ідентифікації за геометрією обличчя;
- аналіз методів біометричної ідентифікації;
- аналіз середовища розробки;
- аналіз існуючих розробок;
- аналіз інструментів та засобів розробки додатків;
- розробку моделі ідентифікації обличчя користувача;
- розробку програмне забезпечення.

В даній магістерській кваліфікаційній роботі аналізується та вирішується проблема біометричної ідентифікації обличчя користувача на основі антропометричних показників вказаного суб’єкта, шляхом розробки

комп’ютерної системи на основі нейромережевого підходу. В процесі розробки були досягнуті наступні результати:

1) Розроблено архітектуру нейронної мережі для розпізнавання та ідентифікації об’єктів на основі індивідуальних антропометричних параметрів обличчя користувача.
2) Розроблено моделі та методи для побудови математичних моделей ідентифікації антропометричних показників користувача на основі технологій нейромереж.
3) Проведені експериментальні дослідження отриманої системи ідентифікації, які доводять про перспективність застосунку як технології біометричної ідентифікації обличчя користувачів.
4) Розроблено комп’ютерну систему, яка є рекомендованою до застосування в корпоративних та приватних умовах з метою ведення обліку за суб’єктами для відслідкування та запобіганню викраденню даних.
5) Було доведено, що одним з важливих способів оптимізації точності розпізнавання розробленої системи ідентифікації нейронних є вдосконалення математичної моделі.
6) Доведено доцільність використання нейронних мереж в задачах біометричної ідентифікації обличчя користувача.

Вивчення показників отриманої комп’ютерної системи дало таку інформацію: Отриманий коефіцієнт помилкової ідентифікації користувачів становить 0,51%, що відповідає встановленим критеріям та є передуючим значенням в порівняні з іншими методами. Як покращення отриманих результатів можна провести збільшення розміру вибірки, розширення її репрезентативності, покращення можливостей апаратного забезпечення та зміна політики обмеження часу навчання нейромережі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Downes S., Muirhead B. Authentication and identification. National Research Council Canada, 2005.
2. Evolution of Authentication Mechanisms. URL: https://ijcsmc.com/docs/papers/November2013/V2I11201351.pdf (дата звернення: 05.10.2022).
3. Improving customer authentication. URL: https://www.atlantafed.org/-/media/Documents/rprf/rprf_pubs/improving-customer-authentication.pdf (дата звернення: 05.10.2022).
4. A Review on Authentication Methods. URL: https://hal.archives-ouvertes.fr/hal-00912435/PDF/A_Review_on_Authentication_Methods.pdf (дата звернення: 05.10.2022).
5. A practical guide to biometric security technology. URL: https://cedar.buffalo.edu/~govind/CSE717/papers/PracticalGuide.pdf (дата звернення: 05.10.2022).
6. Biometrics: the future of identication. URL: http://web.cse.msu.edu/~jain/BiometricsTheFutureOfIdentification.pdf (дата звернення: 05.10.2022).
7. Global Biometrics Technology Market: By Type: Face, Hand Geometry, Voice, Signature, Iris, AFIS, Non-AFIS. URL: https://www.expertmarketresearch.com/reports/biometrics-market (дата звернення: 05.10.2022).
8. Wayman L., A definition of biometrics. National Biometric. Jose State University, 2000.
9. Daugman J., Biometric decision landscapes. University of Cambridge Computer Laboratory, 1999.
10. Дворянкин С. Мовний підпис. Москва, 2003.
11. Методи біометричної автентифікації. URL: http://www.msiit.ru/x/miszki/_4___.html (дата звернення: 05.10.2022).
12. Human and machine recognition of faces: a survey. URL: https://engineering.purdue.edu/~ece624/papers/challapa_facerecognition.pdf (дата звернення: 05.10.2022).
13. Turk M., Pentland A. Face recognition using eigenfaces, in: Proc. Internat. Conf. Pattern Recognition. Hawaii, 1991.
14. Robust face identification scheme: KL expansion of an invariant feature space URL: https://ui.adsabs.harvard.edu/abs/1992SPIE.1607...71A/abstract (дата звернення: 05.10.2022).

15. Support Vector Machines: Theory and Application. URL: https://www.researchgate.net/publication/221621494_Support_Vector_Machines_Theory_and_Applications (дата звернення: 05.10.2022).
16. Face Recognition using Deep Neural Network Technique URL: https://www.researchgate.net/publication/336472561_Face_Recognition_using_Deep_Neural_Network_Technique (дата звернення: 05.10.2022).
17. Fundamental Concepts of Convolutional Neural Network URL: https://www.researchgate.net/publication/337401161_Fundamental_Concepts_of_Convolutional_Neural_Network (дата звернення: 05.10.2022).
18. An Introduction to Autoencoders URL: https://arxiv.org/pdf/2201.03898.pdf (дата звернення: 05.10.2022).
19. Facial component-landmark detection URL: https://www.researchgate.net/publication/224238143_Facial_component-landmark_detection (дата звернення: 05.10.2022).
20. A Few Useful Things to Know About Machine Learning URL: https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf (дата звернення: 05.10.2022).
21. Comparison between Euclidean and Manhattan distance measure for facial expressions classification URL: https://www.researchgate.net/publication/317244989_Comparison_between_Euclidean_and_Manhattan_distance_measure_for_facial_expressions_classification (дата звернення: 05.10.2022).
22. Raja R. Face Detection Using OpenCV and Python URL: https://www.superdatascience.com/opencv-face-detection/ (дата звернення: 05.12.2022).
23. Limitations of Deep Neural Networks URL: https://arxiv.org/ftp/arxiv/papers/2012/2012.15754.pdf (дата звернення: 05.12.2022).
24. Identification in Organizations URL: https://www.researchgate.net/publication/234021306_Identification_in_Organizations_An_Examination_of_Four_Fundamental_Questions (дата звернення: 05.12.2022).
25. A Comparative Study of Neural Network Models for Sentence Classification URL: https://arxiv.org/pdf/1810.01656.pdf (дата звернення: 05.12.2022).

26. Dynamical Variational Autoencoders URL: https://hal.inria.fr/hal-02926215/file/Girin_at_al_DVAE_review_2021_arXiv_version.pdf (дата звернення: 05.12.2022).
27. Graph Anomaly Detection with Deep Learning URL: https://arxiv.org/pdf/2106.07178.pdf (дата звернення: 05.12.2022).
28. Inception-ResNet URL: https://arxiv.org/pdf/1602.07261.pdf (дата звернення: 05.12.2022).
29. Hebb, D., Muirhead B. The organization of behavior; a neuropsychological theory. New York, 1949.
30. Variational Autoencoders URL: https://arxiv.org/pdf/1906.02691.pdf (дата звернення: 05.12.2022).
31. Generative Adversarial Networks URL: https://arxiv.org/ftp/arxiv/papers/2005/2005.13178.pdf (дата звернення: 05.12.2022).
32. Auto-Encoding Variational Bayes https://arxiv.org/pdf/1312.6114.pdf (дата звернення: 05.12.2022).
33. Multimodal hierarchical Variational AutoEncoders URL: https://arxiv.org/pdf/2207.09185.pdf (дата звернення: 05.12.2022).
34. iBUG 300-W data collection URL: https://ibug.doc.ic.ac.uk/resources/facial-point-annotations/ (дата звернення: 05.12.2022).
35. ResNet-50 Convolutional Neural Network URL: https://aclanthology.org/2021.sigtyp-1.13.pdf (дата звернення: 05.12.2022).
36. Stacked Hourglass Networks URL: https://arxiv.org/pdf/1603.06937.pdf (дата звернення: 05.12.2022).
37. The Own-Race Bias for Face Recognition in a Multiracial Society URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00208/full (дата звернення: 05.12.2022).
38. Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks URL: https://arxiv.org/ftp/arxiv/papers/1604/1604.02878.pdf (дата звернення: 05.12.2022).

39. Efficient Non-Maximum Suppression URL: https://www.researchgate.net/publication/220929789_Efficient_Non-Maximum_Suppression (дата звернення: 05.12.2022).
40. Deep Residual Learning for Image Recognition URL: https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/He_Deep_Residual_Learning_CVPR_2016_paper.pdf (дата звернення: 05.12.2022).
41. VGG Face Dataset URL: https://www.robots.ox.ac.uk/~vgg/data/vgg_face/ (дата звернення: 05.12.2022).
42. Система розпізнавання обличчя URL: https://nure.ua/wp-content/uploads/2020/Konkurs/17-sistema.pdf (дата звернення: 05.12.2022).
43. Detecting Faces in Images: A Survey URL: https://www.researchgate.net/publication/3193340_Detecting_Faces_in_Images_A_Survey (дата звернення: 05.12.2022).
44. DLIB library URL: http://dlib.net/ (дата звернення: 05.12.2022).
45. OpenCV library URL: https://opencv.org/ (дата звернення: 05.12.2022).
46. PyTorch framework URL: https://pytorch.org/ (дата звернення: 05.12.2022).
47. TensorFlow framework URL: https://www.tensorflow.org/ (дата звернення: 05.12.2022).
48. Reducing false rejection rate in iris recognition by quality enhancement and information fusion URL: https://core.ac.uk/download/pdf/230460611.pdf (дата звернення: 05.12.2022).
49. Visualizing Data using t-SNE URL: https://www.jmlr.org/papers/volume9/vandermaaten08a/vandermaaten08a.pdf (дата звернення: 05.12.2022).
50. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.
51. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа – Вінниця : ВНТУ, 2016. – 113 с.

Додаток А. Результат перевірки роботи на плагіат

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 2. Модуль ідентифікації.

Автор роботи: Кулик Леонід Русланович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 98,3%. Схожість – 1,7%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Кулик Л. Р.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Кавацюк Н. Р.
(підпис) (прізвище, ініціали)

ІЛЮСТРАТИВНИЙ МАТЕРІАЛ

ЗАГАЛЬНА СТРУКТУРА СИСТЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ОБЛИЧЧЯМ

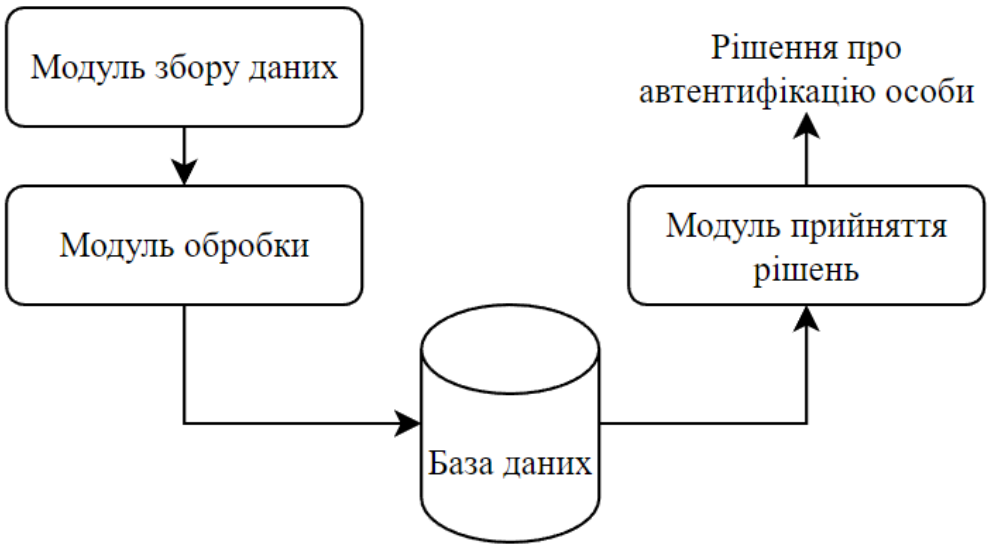


СХЕМА ПРОЦЕСУ ОТРИМАННЯ ВЕКТОРА УНІКАЛЬНИХ ХАРАКТЕРИСТИК

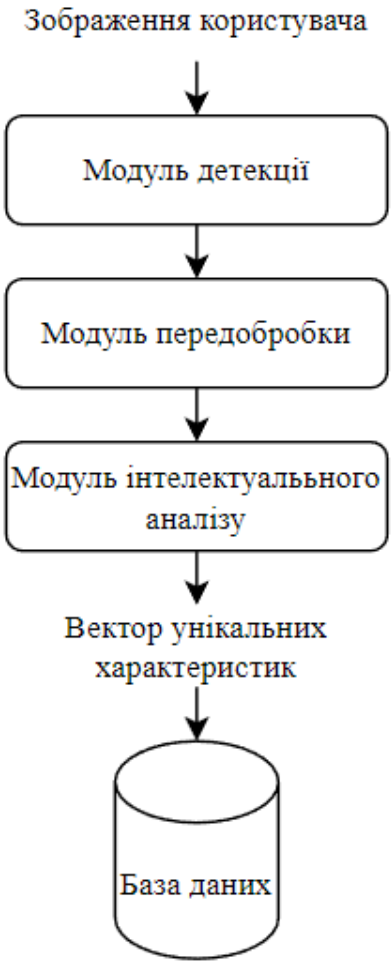
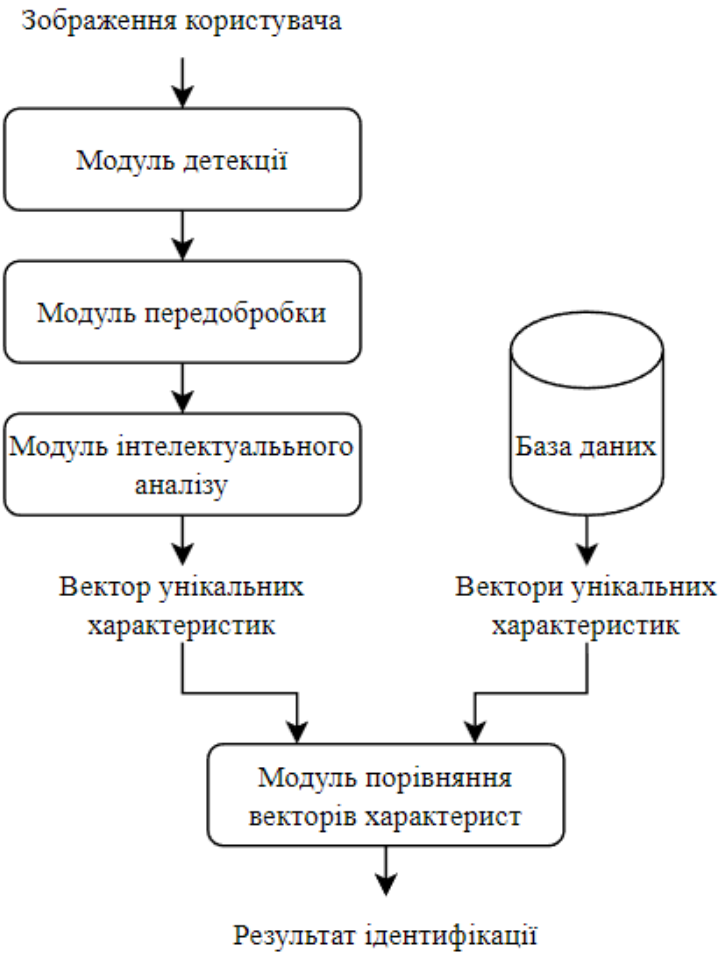
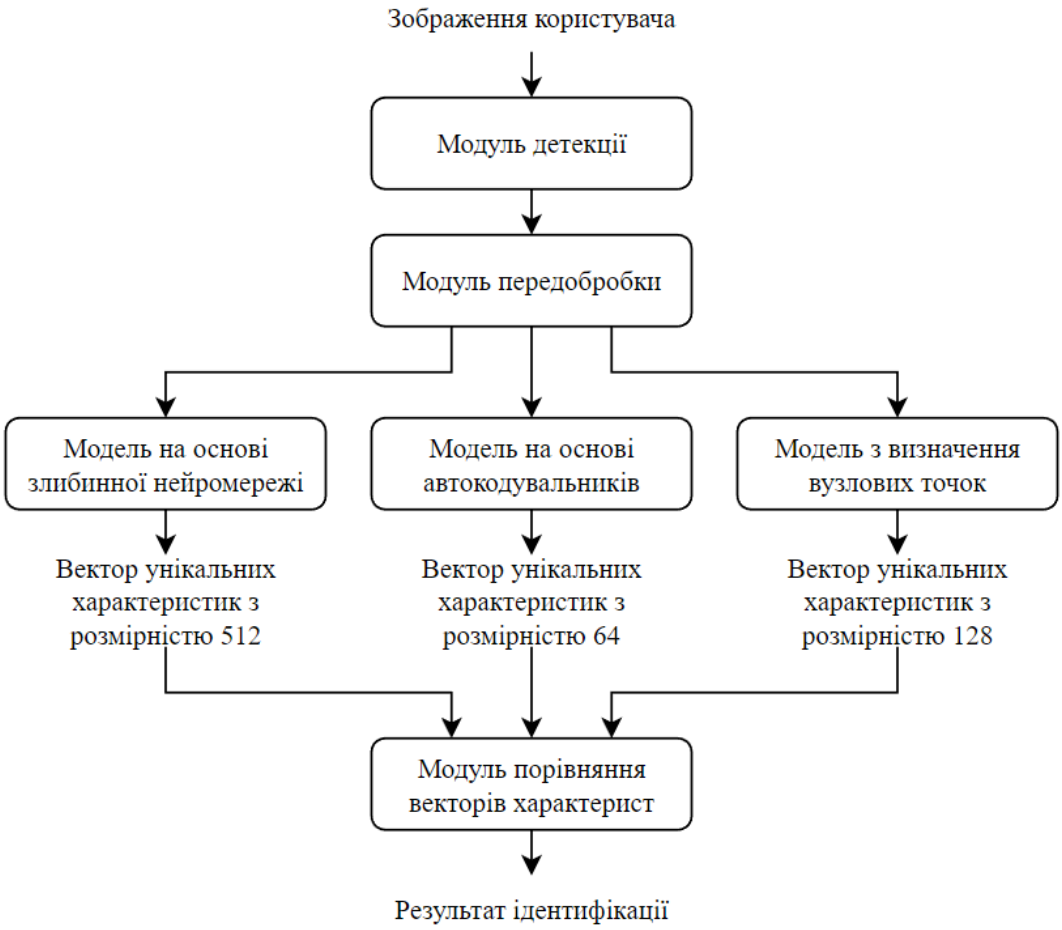


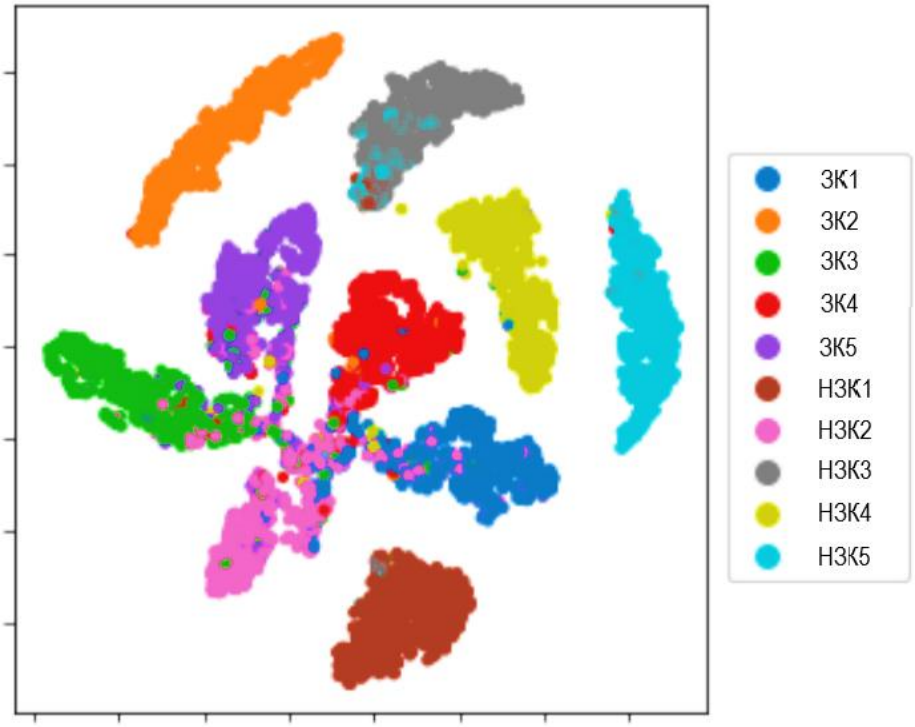
СХЕМА ПРОВЕДЕННЯ ПЕРЕВІРКИ ЗОБРАЖЕНЬ КОРИСТУВАЧА В ПРОЦЕСІ РОБОТИ



СТРУКТУРА МОДЕЛІ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧА



ДІАГРАМА ВИХІДНИХ ВЕКТОРІВ ХАРАКТЕРИСТИК ДЛЯ МОДЕЛІ НА ВУЗЛОВИХ ТОЧКАХ



ГРАФІК ЗАЛЕЖНОСТІ ПОКАЗНИКІВ FAR ТА FRR ВІД КІЛЬКОСТІ ПОМИЛОК ПРИ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧА ДЛЯ МОДЕЛІ НА ВУЗЛОВИХ ТОЧКАХ