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 1. Модуль детекції»

08-20.МКР.013.00.000 ПЗ

Виконав: студент 2 курсу, групи 1БС-21м
спеціальності 125 Кібербезпека
_____ Говорун В. В.

Керівник: к. т. н., доц. каф ЗІ
_____ Дудатьєв А. В.
«19» грудня 2022 р.

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

Допущено до захисту

Завідувач кафедри ЗІ, д.т.н., проф
_____ Лужецький В. А.
«19» 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
«13» 09 2022 року

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

Говорун Володимиру Валерійовичу

1. Тема роботи: «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 1. Модуль детекції»
керівник роботи: Дудатьєв Андрій Веніамінович, к. т. н., доц. 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 – Windows;
– розробка ізольованих модулів для детекції користувача;
– середовище розробки – WebStorm;
– мова програмування – JavaScript;

4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Методи та моделі для детекції. 3. Реалізація системи детекції користувача. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.

5. Перелік графічного матеріалу: Структура моделі детекції обличчя користувача (плакат, А4). Загальна архітектура системи ідентифікації користувача за обличчям (плакат, А4). Загальний вигляд моделі ідентифікації обличчя користувача (плакат, А4). Блок схема роботи процесу детекції (плакат, А4). Блок схема роботи модулю попередньої обробки зображення (плакат, А4). Структура подвійного blaze блоку (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Дудатьєв А. В., к.т.н., доц. каф. ЗІ		
2	Дудатьєв А. В., к.т.н., доц. каф. ЗІ		
3	Дудатьєв А. В., к.т.н., доц. 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 обгрунтування	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 – 08.10.2022	
6	Розробка рішень, моделей, алгоритмів	09.10.2022 – 16.10.2022	
7	Тестування розробленого ПЗ	17.10.2022 – 14.11.2022	
8	Розробка розділу економічного обгрунтування доцільності розробки	15.11.2022 – 17.11.2022	
9	Аналіз виконання ТЗ, висновки	18.11.2022 – 21.11.2022	
10	Оформлення пояснювальної записки	22.11.2022 – 24.11.2022	
11	Перевірка магістерської роботи на наявність плагіату	25.11.2022 – 29.11.2022	
12	Попередній захист та доопрацювання МКР	30.11.2022 – 02.12.2022	
13	Предетавлення МКР до захисту, рецензування	07.12.2022 – 19.12.2022	
14	Захист МКР	20.12.2022 – 21.12.2022	
16	Аналіз завдання. Вступ	22.12.2022 – 26.12.2022	

Студент _____ (підпис) Говорун В. В

Керівник роботи _____ (підпис) Дудатьєв А. В

АНОТАЦІЯ

УДК 681.325.5

Говорун В. В. Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем. Частина 1. Модуль детекції.

Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2022. 99 с.

На укр. мові. Бібліогр.: 35 назв; рис.: 37; табл. 18.

Магістерська кваліфікаційна робота присвячена розробці моделей та методів для детекції обличчя користувачів комп'ютерних систем. Під час виконання магістерської кваліфікаційної роботи для розв’язання поставленої задачі було здійснено аналіз існуючих видів біометричної ідентифікації та методів їх реалізації, а також методів детекції обличчя, основні типи нейронних мереж і досліджено переваги та недоліки біометричної ідентифікації порівняно з іншими типами ідентифікації.

Розробка програми виконана в середовищі WebStorm за допомогою мови програмування JavaScript. Розроблено модуль для детекції користувача. На основі отриманих даних було проведено тестування нейронної мережі для вирішення завдання. Реалізовано і протестовано засіб, який виконує детекцію обличчя користувача.

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, детекція обличчя, нейронна мережа.

ABSTRACT

Hovorun V. V. Models and methods for detection and identification of faces of computer users. Part 1. Detection module.

Master's thesis on specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2022. 99 p.

In Ukrainian speech Bibliography: 35 titles; Fig.: 37; table 18.

The master's thesis is devoted to the development of models and methods for face detection of computer system users. During the performance of the master's qualification work to solve the task, an analysis of existing types of biometric identification and methods of their implementation, as well as methods of face detection, the main types of neural networks, and the advantages and disadvantages of biometric identification compared to other types of identification were investigated.

The program was developed in the WebStorm environment using the JavaScript programming language. A module for user detection has been developed. Based on the obtained data, neural network testing was conducted to solve the problem. Implemented and tested a tool that detects the user's face.

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, face detection, neural network.

ЗМІСТ

ВСТУП

В епоху інтернету фундаментальні права користувачів на конфіденційність і анонімність привернули значну увагу досліджень. Це не лише результат експоненційного зростання даних, які користувачі генерують під час виконання своїх щоденних завдань за допомогою обчислювальних пристроїв із розширеними можливостями, але й через властиві даних характеристики, які дозволяють пов’язувати їх із користувачем. Постачальники послуг використовують ці факти для моніторингу та ідентифікації користувачів, хоча й впливають на анонімність користувачів, в основному на основі особистої ідентифікаційної інформації або датчиків, які генерують унікальні дані для надання персоналізованих послуг. Загальні результати показують, що за певних конфігурацій анонімність користувачів може бути збережена, тоді як в інших випадках ідентифікація користувачів може бути зроблена з високою точністю, не покладаючись на особисту ідентифікаційну інформацію.

Поширення онлайн-додатків і послуг, доступних для кінцевих користувачів, у поєднанні з їх безперервним, високочастотним використанням призвело до різкого збільшення кількості даних, створених користувачами, які підлягають моніторингу та запису. Цей постійно зростаючий обсяг дуже детальних даних, які стосуються особистої та приватної діяльності користувачів, становить великий ризик для конфіденційності користувачів, оскільки їх можна використати для потенційного розкриття їхньої діяльності та загрози їхній анонімності.

Це в свою чергу, зробило проблему розмежування доступу до інформації та безпечним володінням нею, одним із найважливіших питань сьогодення. Тому дослідження проблеми інформаційної безпеки, яка в свою чергу зобов’язана забезпечувати конфіденційність інформації, доступність інформації для користувачів, які мають права доступу до неї, захищеність інформації від несанкціонованих модифікацій та руйнування, є як ніколи актуальним.

Існуючі традиційні методи ідентифікації, такі як звичайні паролі, смарт-картки, токени, ті інші різноманітні електронні ключі, володіють дуже критичними недоліками, а саме це можливість їх підробки, викрадення або зламу. Проте для вирішення, цих проблем може бути використана біометрія, яка дозволяє одночасно визначати суб'єкт доступу та повноваження користувача відносного цього ресурсу.

Принцип роботи методів ідентифікації за допомогою біометрії полягає в тому що із об'єкта за допомогою біометричних датчиків "витягуються" певні характеристики, які потім відсилаються процесору, за для їх аналізу та виявлення і виділення відмінні від інших характеристик, при цьому відкидаючи усі інші. Далі за допомогою цих оброблених біометричних зразків, формуються певні шаблони, які зберігаються в базі даних, і потім порівнюються, при процесі ідентифікації користувача. Такий метод ідентифікації, на сьогодні можна назвати одним із найефективніших та зручних методів для ідентифікації користувача.

Проте і у таких методів, є свої певні недоліки, і вони при всій своїй ефективності та надійності, не можуть гарантувати сто відсоткову правильність ідентифікації особи. Як варіантом вирішення цієї проблеми, може бути використання певного інтегрованого підходу, який буде поєднувати декілька методів разом, що в свою чергу зможе підвищити точність та правильність ідентифікації в цілому.

Об'єктом дослідження є детекція обличчя користувачів.

Предметом є моделі та методи детекції обличчя користувача за допомогою його біометричних характеристик.

Метою магістерської кваліфікаційної роботи є вдосконалення існуючих моделей та методів детекції обличчя користувача за допомогою нейронних мереж.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– проаналізувати вибірку даних та на основі аналізу створити модель;

– дослідити існуючі моделі для детекції обличчя користувача;

– проаналізувати існуючі методи детекції обличчя користувача;

– розробити модуль для детекції обличчя користувача за допомогою нейромереж;

– розробити модуль для передачі характеристик обличчя користувача в модуль його подальшої ідентифікації;

– обрати засоби реалізації програмного засобу;

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

– розробити та протестувати засіб на основі поставленої задачі.

Наукова новизна роботи полягає в наступному: було проведено комплексний аналіз та класифікацію методів та алгоритмів виділення об’єктів на цифрових зображеннях, що надало можливість підкреслити їх переваги та недоліки, а також розробити власний алгоритм детекції обличчя користувача, за допомогою використання сучасних нейронних мереж, що в свою чергу дозволило зменшити обчислювальну складність процесу детекції в цілому та підвищити ефективність та швидкість його роботи.

Практична цінність полягає у тому, що розроблено застосунок, який в повній мірі реалізує розроблений метод детекції обличчя користувача, та може бути використаний в подальшому в системах для ідентифікації користувача на основі його біометричних даних. Низька обчислювальна складність роботи методу дозволяє, подальше створення застосунку для його роботи на мобільних пристроях.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз методів ідентифікації користувача

На сьогоднішній день, поява нових та сучасних засобів для зберігання, обробки і передачі даних в свою чергу призвело до відкриття принципово нових можливостей їх використання в найрізноманітніших сферах людської діяльності. Проте не вся інформація, є публічною та відкритою для доступу, її конфіденційне зберігання в комп’ютерних мережах зазвичай пов'язано з необхідністю розмежування доступу до неї та ідентифікації користувачів, які роблять цей запит.

Всі наявні на даний час способи ідентифікації користувача [1] можна розділити на наступні:

– ідентифікація по паролю;

– ідентифікація із застосуванням спеціалізованих пристроїв (smart-card, touch-memory, тощо);

– ідентифікація за біометричними характеристиками користувача (аналіз відбитка пальця, сітківки ока, почерку, голосу і т д.

– комплексні системи ідентифікації;

Ідентифікація за допомогою паролю, раніше була ледве не одним способом для визначення того, ким саме є поточний користувач. Причиною цього є те, що вона досить як у використанні, так й у її реалізації. Вся її сутність зводиться до того, що кожен зареєстрований користувач певної системи отримує набір певних даних(зазвичай це пара логін та пароль).

Потім під час наступних кожних входах в систему, користувач вказує свої дані, і системи вже в свою чергу на основі ідентифікує користувача, як певну особистість, на основі унікальності наданих йому даних, що означає, що в системі не може існувати ще один користувач, з такою самою ідентичною парою логіна і пароля.

До переваг такого методу можна віднести саме його простоту у використанні та при реалізації, такого методу в системі. Проте нажаль в такого

методу, є досить багато недоліків, а саме це – його надійність, оскільки пару логін та пароль, при їх недостатній складності, запросто може підібрати зловмисник, що може в свою чергу завдати серйозного удару по безпеці такої системи.

Апаратна ідентифікація заснована на визначенні особистості користувача за допомогою стороннього предмета або ключа, що перебуває в його користуванні. Звичайно, мова йде не просто звичайні металеві ключі, а про спеціальні електронні пристрої. Найбільш популярними з них на сьогодні є смарт картки, та токени.

З переваг ідентифікації за допомогою такого методу, є досить висока надійність, оскільки на відміну від парольної ідентифікації, такий метод не буде зламаний, оскільки має певну стійкість до зламу. Проте і в такого методу на жаль, є свої досить вагомі недоліки, а саме це - ціна, оскільки смарт картки, з високою стійкістю до зламу, коштують досить дорого, і самий факт того, що смарт карта або токен, може бути просто викрадений в користувача зловмисником.

Ідентифікація та автентифікація є надзвичайно важливими завданнями, оскільки ми продовжуємо рухатися в більш орієнтовану на інформацію епоху. Автентифікація стає необхідною для двох основних пристроїв, якими сьогодні користуються майже всі, тобто ноутбуків/нетбуків і мобільних телефонів. Ідентифікація стає дедалі складнішою проблемою, оскільки стає доступним усе більше методів підробки особи.

Протягом кількох десятиліть дослідники вдосконалювали біометричні методи та намагалися знайти різні параметри людського тіла або поведінкові методи, які є унікальними для людини, щоб їх можна було застосувати в групі людей (вибірці) для диференціації та ідентифікації одиничного людини, отримуючи найвищу точність і швидку відповідь.

Загалом можна сказати, що біометрія шукає дані, які не змінюються протягом вашого життя або які важко підробити чи змінити навмисно.

Щоб біометрія була успішною, необхідно мати принаймні такі характеристики:

– характеристики не повинні змінюватися протягом життя людини;
– характеристики мають однозначно ідентифікувати особу;
– характеристики повинні легко скануватися або читатися;
– необхідне обладнання не повинно бути занадто дорогим;

Щоб сказати, що біометричну систему впроваджено добре, є фактори, які слід брати до уваги, наприклад час відгуку, вартість, точність тощо. Вони залежать від апаратного забезпечення, а також від програмного забезпечення. Однак біометрична ідентифікація стає звичним явищем, оскільки обладнання та програмне забезпечення падають у ціні.

Використання біометрії є одним із потенційних (або часткових) рішень проблем ідентифікації та автентифікації, оскільки системи, які засновані на її використанні, окрім своєї високої ефективності, достовірності та зручності в користуванні, мають ще досить серйозну перевагу в тому, що на відміну звичайних способів ідентифікації із використанням додаткових пристроїв та способів ідентифікації за допомогою пароля, не вимагають від користувача завжди мати при собі якийсь «ключ», оскільки сам факт існування такого ключа, створює певну ймовірність того, що він може бути викрадений зловмисником або підроблений. В біометричних системах в свою чергу під час ідентифікації, «ключем» завжди є сам користувач, що виключає ймовірність втрати або викрадення цього ключа.

Загалом всі системи для ідентифікації користувача за допомогою біометрії поділяються на два основних класи:

– ті, які в своїй основі використовують аналіз певних статичних параметрів;

– ті, які в своїй основі використовують аналіз певних динамічних параметрів користувача;

Методи біометричної ідентифікації на основі статичних параметрів користувача, опираються на невід'ємні фізіологічні характеристики, що надані

йому з народження. До цих методів можна віднести: аналіз відбитків пальців, форми долоні, форми обличчя, форми руки, і т.д.

Методи біометричної ідентифікації на основі динамічних параметрів користувача, опираються на поведінкову характеристику людини , тобто вони в свою чергу побудовані на особливостях, що характерні для підсвідомих рухів у процесі якої-небудь дії. Динамічні біометричні процедури ідентифікації особистості ґрунтуються на аналізі підписів , особливостей голосу , клавіатурного почерку , інших ознаках складних підсвідомо керованих рухів.

Цікавою рисою систем динамічної ідентифікації є те , що вони здатні паралельно з ідентифікацією оцінювати поточний психічний стан особистості . Динаміка підпису та динаміка відтворення голосом ключової фрази істотно змінюється , наприклад , при сп'янінні або при попаданні особистості в стресовий стан. З цієї причини динамічні методи розглядається як психологічні [2]. В наступному розділі буде розглянуто більш детально кожну із цих груп, та методи, які вони в себе включають.

1.2 Огляд сучасних методів біометричної ідентифікації користувача

На сьогоднішній день біометрія, як наукова дисципліна має ряд практично незалежних один від одного напрямків, кожний з яких має свої особливості та характеристики. У дослідженнях по біометричній тематиці активну участь беруть десятки наукових центрів при університетах ряд перспективних організацій комерційних фірм.

Біометрія успішно переконала широкий спектр додатків прийняти не лише як фундаментальний компонент у їхній архітектурі безпеки, але й як економічний інструмент, який може призвести прямо чи опосередковано до економії витрат і зменшення фінансових ризиків [3].

За два десятиліття ринок біометрії швидко і значно просунувся вперед. Оскільки порівнюючи з іншими методами ідентифікації, біометрія має великий

перелік переваг, а саме – підвищену безпеку, зручність, досить високу точність та надійність.

Останні дослідження підтверджують, що ринок біометрії зросте з 8,7 мільярдів доларів у 2013 році до майже 27,5 мільярдів доларів у 2019 році, зареєструвавши щорічне зростання на 19,8% між 2014 та 2019 роками, див. рисунок 1.1.

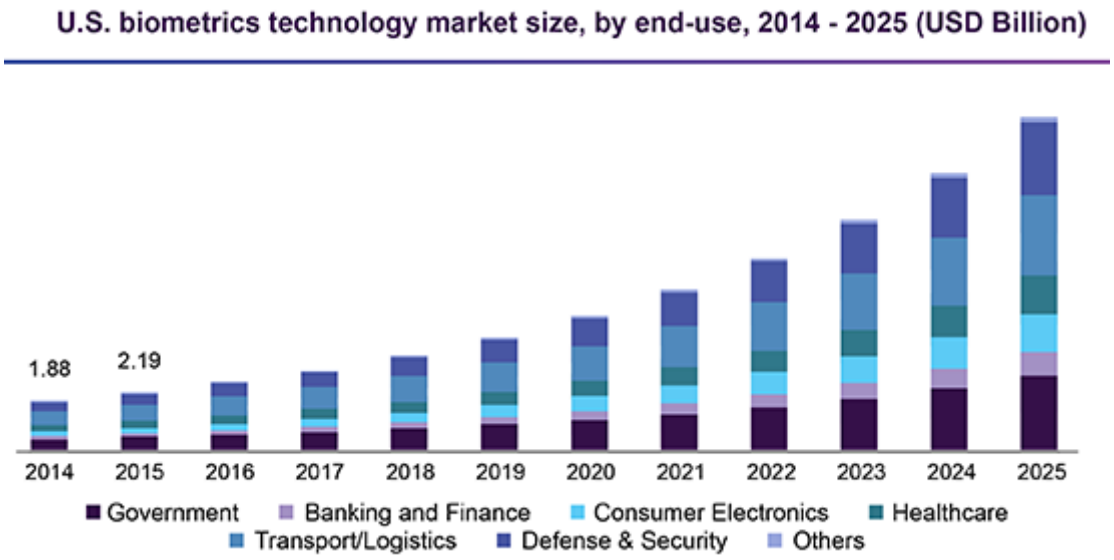


Рисунок 1.1 – Графік зростання ринку біометричних технологій

Модальність відбитків пальців все ще домінуватиме на ринку, як показано на рисунку 1.2.

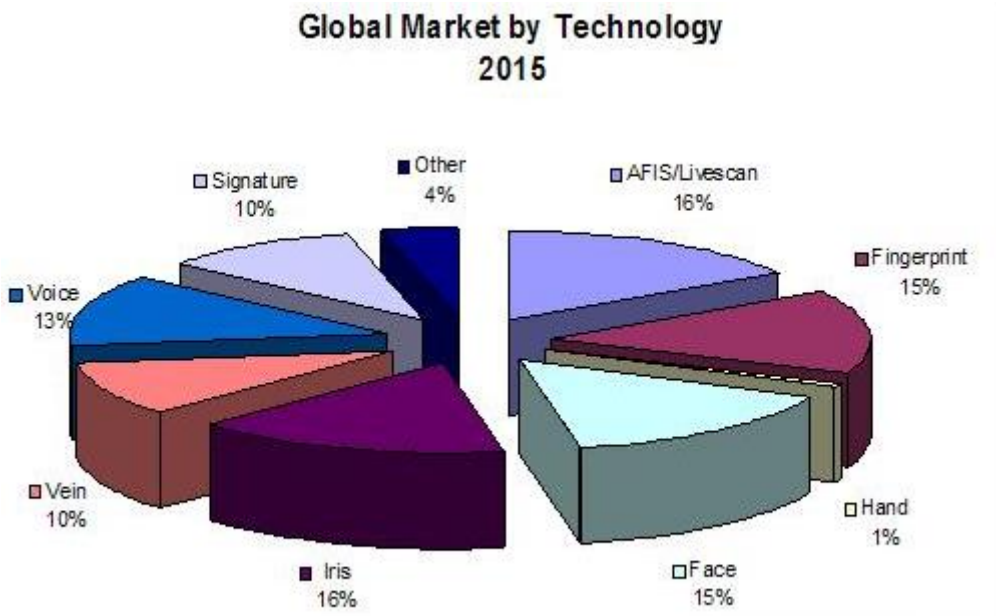


Рисунок 1.2 – Розподіл технологій на ринку біометрії

Це прискорення виправдане поширенням електронних послуг, що вимагає ідентифікації разом зі зростанням шахрайства та крадіжок особистих даних, з якими потрібно боротися. Крім того, впровадження електронних документів, особливо біометричних паспортів та національних ідентифікаційних карток, великими урядами сприятиме значному розширенню їх використання.

Зараз біометрія досить широко використовується у наступних галузях:

– державні документи - біометричне національне посвідчення особи, біометричний паспорт, кордон контроль, соціальний захист, електронне голосування;

– контроль доступу - він може бути фізичним, наприклад системами обліку робочого часу та безпеки дверей, або логічним, таким як доступ до ресурсів віддаленого комп’ютера та інформаційних систем;

– мобільні програми - останні мобільні телефони оснащені біометричними технологіями, які дозволяють ідентифікація власника, розблокування пристрою, здійснення комерційних операцій і т. д. Для наприклад, Apple iPhone 5s і Samsung Galaxy A5 поставляються з вбудованим відбитком пальця рідер разом із інтелектуальним програмним забезпеченням, які призначені для розпізнавання;

– комерційні програми - більшість продуктів інтегрують біометричні дані для покращення користувацьких досвід. Доступ до комп’ютерів, інтернет-додатків, електронної комерції, банківських операцій, тощо

– криміналістичні програми - судово-медичні лабораторії зазвичай використовують біометричні дані у своїх кримінальних справах розслідування та встановлення батьківства, а також для ідентифікації трупів. Нові дослідження підтвердили можливість визначення походження предка людини за його відбитком пальця;

– військове застосування - це включає системи ідентифікації для використання в польових умовах, контроль доступу і моніторинг додатків у чутливих областях, а також розгортання великих баз даних;

Існуючі продукти слід розділити на дві гілки. До першої потрібно віднести велику групу біометричних продуктів побудованих на аналізі статичних (незмінюваних) особливостей користувача, наданих йому від народження і добре спостережуваних оточуючими. Прикладами такого типу біометричних продуктів можна навести такі пристрої, що побудовані на аналізі особливостей рис обличчя, геометрії рук та відбитків пальця .

До другої, принципово іншої гілки біометричних продуктів слід віднести пристрої біометричної ідентифікації, що в свою чергу побудовані на аналізі динамічних зразків особистості [5]. Динамічні образи особистості відображають особливості характерних для неї швидких рухів в процесі відтворення контрольного слова рукописним почерком, набору тексту на

Особливість ідентифікації за біометричними параметрами базується на їх винятковості. Ймовірність того, що знайдуться дві людини з однаковими ознаками, дуже мала (наприклад, ймовірність того, що в двох різних людей на однакових пальцях однієї руки збігатимуться відбитки пальців, рівна 1/24 млн, тобто практично є нульовою).

Існують наступні види біометричної ідентифікації:

1) Розпізнавання обличчя:

Ідентифікація людини за зображенням обличчя може бути виконана різними способами, наприклад, за допомогою захоплення зображення обличчя у видимій спектрі за допомогою недорогої камери або за допомогою інфрачервоних візерунків обличчя (тепло - випромінювання).

Розпізнавання обличчя у видимому світлі, як правило, моделює основні особливості з центральної частини зображення обличчя.

Використовуючи широкий асортимент камер системи витягують функції особливості з захоплених зображень, які не змінюються з часом, уникаючи поверхневих ознак, таких як міміка людини або її волосся.

Кілька підходів до моделювання зображення обличчя у видимій спектрі є основними - аналіз компонентів, локальний аналіз функцій, використання

нейронних мережі, теорія еластичних графів та аналіз багатогранної роздільної здатності.

Деякі з проблем розпізнавання обличчя у візуальному вигляді спектру включають зменшення впливу змінного освітлення та виявлення маски або фотографії. Деяким системам для розпізнавання обличчя може знадобитися нерухомий або спеціально позиціонований користувач, для захоплення його зображення, хоча багато систем використовують режим реального часу для виявлення голови людини та автоматичного пошуку обличчя. Основні переваги біометричної ідентифікації за допомогою розпізнавання обличчя полягають у тому, що такий процес є ненав'язливим, безперервним і досить зручним для більшості користувачів, оскільки не потребує від них багато взаємодії [4].

2) Розпізнавання голосу

Розпізнавання голосу має історію, що датується чотирма десятиліттями, де вихід декількох аналогових фільтрів усереднювався з часом для узгодження. Розпізнавання голосу використовує акустичні особливості мови, які, як було встановлено, відрізняються між людьми. Ці акустичні зразки відображають як анатомію (наприклад, розмір і форму горла та рота), так і вивчені поведінкові зразки (наприклад, голосовий крок, стиль розмови).

Це включення вивчених шаблонів у шаблони голосу (останні під назвою "Голосові відбитки") заслужило розпізнавання оратора, яка його класифікація як "поведінкова біометрична". Системи розпізнавання голосу використовують три стилі розмовного введення: залежний від тексту, частково залежний від тексту та незалежний від тексту.

Більшість програм для розпізнавання голосу передбачають як вхідні дані, специфічний текст, який передбачає вибір та зарахування одного або декількох голосових паролів. Різні технології, що використовуються для обробки та зберігання голосових відбитків, включають приховані моделі Маркова, алгоритми відповідності шаблонів, нейронні мережі, представлення матриці та дерева рішень. Зниження продуктивності роботи такого методу ідентифікації може бути результатом змін у власних атрибутах голосу та від отримання набору

даних користувача за допомогою його записів з одного телефону і подальшій ідентифікації його вже через інший телефон. Також при використанні такого методу потрібно звернути увагу на такий фактор, як зміна голосу внаслідок старіння, оскільки це може спричинити помилку першого роду, для справжнього користувача.

До переваг такого методу ідентифікації можна віднести відносно невелику ціну за необхідне для роботи обладнання, та досить непогану зручність оскільки існуючі мікрофони та технології передачі голосу, що дозволяють якісно передавати голос на великі відстані через звичайні телефони (дротяна лінія або бездротова).

3) Розпізнавання райдужної оболонки

Цей метод розпізнавання використовує райдужну оболонку ока, яка є кольоровою областю, що оточує зіницю.

Шаблони райдужної оболонки вважаються унікальними, їх отримують за допомогою системи збору зображень на основі відео. Сканування пристроїв IRIS використовується в програмах особистої аутентифікації протягом декількох років.

Системи, засновані на розпізнаванні райдужної оболонки, значно знизилися в ціні, і ця тенденція, як очікується, продовжиться. Такий метод досить добре працює як в режимах перевірки та ідентифікації (у системах, що виконують пошук одного до багатьох у базі даних) та має досить високу точність. Поточні системи можна використовувати навіть у присутності окулярів та контактних лінз. Технологія не нав'язливою для користувача, оскільки не вимагає фізичного контакту зі сканером.

4) Геометрія руки та пальців

Такі методи ідентифікації є досить добре розвинуті на даний час. Розпізнавання за допомогою геометрії руки та пальців доступне вже понад двадцять років. Для роботи система може вимірювати або фізичні характеристики пальців, або руки. До них відносяться довжина, ширина, товщина та площа поверхні руки. Однією з цікавих характеристик є те, що деякі

системи потребують невеликого біометричного зразка (кілька байт). Геометрія рук отримала прийняття в різних сферах, її використання можна досить часто помітити у системах контролі фізичного доступу в комерційних та житлових програми, тощо.

5) Розпізнавання підпису

Такий метод використовує динамічний аналіз підпису для ідентифікації людини. Технологія заснована на вимірюванні швидкості, тиску та кута, що використовується людиною, коли виробляється підпис. Одним із фокусів цієї технології були додатки електронного бізнесу та інші програми, де підпис - це прийнятий метод особистої аутентифікації [5].

6) Відбитки пальців

Відбиток пальців - це унікальний спосіб для ідентифікації користувача. Якщо порівняти його з ключем, то можна сказати, що у вас насправді є десять різних унікальних ключів у руках людини, оскільки кожен відбиток пальців відрізняється. Навіть якщо один палець має розріз або вся рука у ранах, все одно буде достатньо пальців для отримання ідентифікації. Відбиток пальців - це дуже певний метод ідентифікації людини, оскільки всі відбитки пальців унікальні. Навіть однакові близнюки мають різні відбитки пальців.

Порівняно з іншими методами ідентифікації, такими як ключ, карта доступу, числовий код або пароль, відбиток пальців дуже безпечний. Оскільки відбиток не можна втратити або забути, і його не можна викрасти, що в свою чергу робить такий метод досить зручним та практичним для користувача.

Таблиця 1 – Переваги та недоліки методів біометричної ідентифікації

Метод	Переваги	Недоліки
Відбитки пальців	- висока точність - зручність - унікальність - стабільність у часі - невелика ціна	- неможливість використання при травмі - сухість шкіри може спричинити ускладнення роботи

Геометрія руки	- невеликий розмір шаблон для роботи - не залежить від стану шкіри	- розмір сканера - низька відмінність
Розпізнавання обличчя	- ефективний процес - висока точність	- зміна обличчя з часом - маніпуляції за допомогою хірургії - не можна розрізнити - між близнюками
Райдужна оболонка ока	- унікальність - висока відмінність - захищеність	- висока вартість - відносно нова технологія
Розпізнавання голосу	- висока точність - не потребує багато взаємодії від користувача	- зміна голосу та мови - через деякий час - легко маніпулювати
Розпізнавання підпису	- унікальність - не потребує багато взаємодії від користувача	- нестабільний у часі - низька відмінність

Таблиця 2 – Характеристика рівнів помилок методів біометричної ідентифікації (помилок першого та другого роду)

Метод	FRR	FAR
Відбитки пальців	(3-7%)	(.001-.01%)
Геометрія руки	(1-2%)	(1-2%)
Розпізнавання обличчя	(10-20%)	(.1-1%)

Райдужна оболонка ока	(2-10%)	>=.001%
Розпізнавання голосу	(10-20%)	(2-5%)
Розпізнавання підпису	(10-20%)	(2-5%)

1.3 Методи біометричної ідентифікації користувача на основі його обличчя

Загалом типову біометричну систему можна описати за допомогою чотирьох основних модулів див. рис. 1.3.

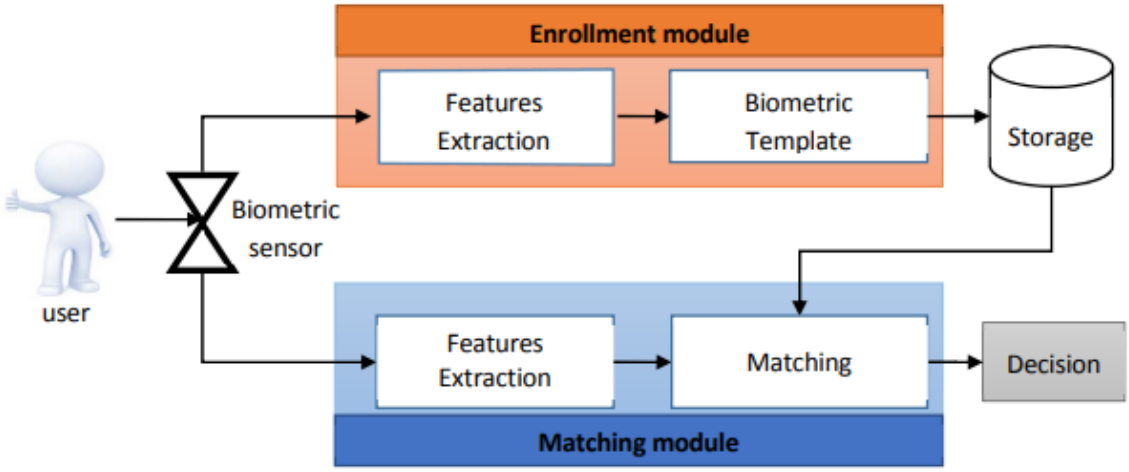


Рисунок 1.3 Типова архітектура біометричної системи

– біометричний датчик - він відповідає за фіксацію біометричних характеристик із біометричного предмета і перетворення його в цифрову форму для передачі в наступні модулі. Продуктивність загального процесу значною мірою залежить від якості отриманих необроблених даних. Насправді ці дані є результатом перетворення реального безперервного явища (наприклад, обличчя) у цифрову таємну форму (зображення обличчя), що іноді може призвести до їх

втрати. Якість отриманих даних залежить від технології зчитувача, доданого шуму та ступеня сумісності користувача з системою;

– реєстрація - отримані необроблені дані спочатку попередньо обробляються для підвищення їх якості. Після того, деякі відповідні дискримінаційні ознаки витягуються підмодулем екстрактора для генерації компактне представлення під назвою «шаблон», яке ефективно відновлює біометричні дані характеристики. Потім створений шаблон надсилається до системи зберігання. Загалом, крок реєстрації дозволяє системі біометричного розпізнавання дізнатися особистість справжні люди в робочому середовищі;

– система зберігання - може бути простим файлом у простій смарт-картці, оскільки це може бути велика база даних, якою керує SGBD (Database System). У зв'язку зі згенерованим шаблоном можна зберігати деякі біографічні відомості (ім'я, паролі, адресу тощо). У будь-якому випадку важливим фактором, з яким потрібно мати справу, є безпека збереженого шаблону. Зламаний шаблон може допомогти відновити оригінальні біометричні характеристики, що становить реальну загрозу;

– модуль відповідності: під час робочої фази системі подається запит на ідентифікацію особи. Він продовжує виділення його дискримінаційних ознак за допомогою підмодуля екстрактора таким же чином, як це було зроблено на етапі реєстрації. Ці витягнуті функції називаються функціями запиту. Після цього збережений шаблон відкликається для порівняння із запитом. Порівняння має на меті підтвердити, що функції запиту та шаблону походять від одного біометричного суб'єкта (особи). Загалом, результатом порівняння є ступінь схожості в діапазоні від 0 (повна невідповідність) до 1 (ідеальний збіг), що дозволяє системі прийняти правильне рішення щодо особи користувача;

З іншого боку, біометрична система може працювати як у режимі перевірки, так і в режимі ідентифікації. У режимі перевірки порівняння виконується лише з одним шаблоном у системі шляхом порівняння 1 до 1.

Це можливо, коли ми хочемо підтвердити особу, заявлену користувачем. У режимі ідентифікації порівняння здійснюється з усіма записами в базі даних шляхом проведення від 1 до багатьох порівнянь. Це той випадок, коли ми хочемо знати, чи особа вже існує в базі даних. Таким чином, система намагається відповісти на питання «хто є користувачем?»

Серед усіх методів біометричної ідентифікації значний інтерес викликають методи, які засновані на розпізнаванні обличчя у зв'язку з дуже низькою потребою дій від користувача та водночас їх зручністю та, відсутністю необхідності придбання додаткового обладнання оскільки у всіх сучасних ноутбуках та телефонах є вбудована камера, якої достатньо для виконання процесу ідентифікації.

Для класифікацій різних існуючих алгоритмів розпізнавання обличчя було запропоновано кілька критеріїв. За принципом роботи методів, або тим, що в них спільного. Найпоширенішим підходом до розпізнавання обличчя є просто обробка зображень обличчя олістичним способом, щоб зафіксувати загальний зв’язок між рисами. З іншого боку, методи, засновані на рисах, зосереджені на розділенні обличчя на важливі окремі риси. У той час як гібридні методи намагаються зробити обидва одночасно та якимось чином поєднати результати. Проте одна проблема під час створення гібридних методів полягає в тому, як їх добре поєднати, щоб отримати найкраще з них обох.

Для цієї роботи було обрано дещо іншу категорію на основі чотирьох груп: це методи проекції, статистики, відповідності графів і нейронних мереж.

Розпізнавання обличчя загалом є проблемою зіставлення шаблонів, що дозволяє розглядати це як проблему зіставлення шаблонів. Чим вищий розмірний простір, тим більше обчислень потрібно для пошуку відповідності.

Іншим важливим аспектом у розпізнаванні обличчя є визначення важливих ознак і представлення класів (осіб) таким чином, щоб можна було вивести оптимальну підмножину, що веде до високої продуктивності класифікації. Це один із факторів появи методів проекції, які в основному намагаються зменшити розміри та використовувати дискримінацію для кращої класифікації.

Статистичні моделі є хорошим способом видалення зайвої інформації та є основною ідеєю 8 статистичних методів, тоді як методи зіставлення графіків були розроблені для кращого моделювання трансформацій облич на зображеннях.

Нейронні мережі широко використовуються в інших сферах, наприклад у машинному навчанні, і можуть ефективно використовуватися для будь-якої складної системи введення - виведення завдяки своїм можливостям навчання.

1.3.1 Проекційні методи

Одним із дуже популярних методів, що лежить в основі багатьох методів проекції для розпізнавання обличчя, є принциповий компонентний аналіз (PCA), який є методом зменшення розмірності. Традиційний алгоритм PCA, використовуваний у підході власних граней Турка та Пентланда [6], обчислює власні вектори та власні значення коваріаційної матриці та вирішує проблему системи власних значень. Цей метод не виконує дискримінації, але замість цього власні вектори, які відповідають найбільшим власним значенням, використовуються як базові вектори в низьковимірному просторі. Зіставлення нової пробної грані потім можна виконати, спроектувавши зображення в цей зменшений простір і знайшовши найближчу відповідність за евклідовою відстанню.

Поєднання власних граней і власних модулів у гібридний метод під назвою модульних власних граней також було перевірено. Результати поєднуються з власних очей, власних носів і власних ротів, які обчислюються на додаток до власних граней аналогічним чином. Через відсутність дискримінації у власних гранях з’явився новий метод, який часто називають лінійним дискримінантом Фішера (FLD), оскільки він заснований на методі Фішера [7].

Його метод, званий лінійним дискримінантним аналізом (LDA), використовується для покращення низьковимірного простору шляхом знаходження найбільш недискримінантних виділених ознак. Цей метод визначає проекцію, яка мінімізує матрицю розсіювання всередині класу і в той же час максимізує матрицю розсіювання між класами. Внутрішньокласове означає

зображення однієї особи, а міжкласове зображення різних осіб, де матриці розсіювання описують відмінності в розкиді даних від середнього значення. Ці методи критерію розрізнення вимагають багатьох навчальних прикладів на обличчя, щоб отримати хороше узагальнення, але є способи штучно збільшити кількість прикладів навіть у невеликому навчальному наборі. Як алгоритм розпізнавання обличчя цей метод називається просто Fisherfaces.

Дуже ефективним методом двійкової класифікації для зіставлення шаблонів загального призначення є опорні векторні машини (SVM), які вперше застосував для розпізнавання облич Філліпс[8]. Вхідні дані проектуються у багатовимірний простір ознак, де відображені дані можуть знову стати лінійно роздільними в перетвореному просторі. Оптимальна гіперплощина визначається шляхом класифікації всіх позитивних і негативних зразків з використанням нелінійної ядерної функції. Цей метод часто використовується в поєднанні з іншими методами для покращення класифікації.

1.3.2 Статистичні методи

Статистичний підхід, також заснований на PCA, його ще можна назвати підходом з ймовірнісними власними гранями [9]. Однак цей метод також використовує розкладання на власний простір для оцінки повних функцій щільності у просторах зображень великої розмірності.

Потім виконується зіставлення з використанням цих оцінок щільності у формулюванні максимальної правдоподібності замість звичайного вимірювання відстані. Іншим методом, подібним до PCA, є аналіз незалежних компонентів (ICA), який намагається оцінити незалежні характеристики об’єктів, наприклад обличчя людей. Бартлет та ін. [10] описує, що існує багато підходів до виконання ICA, і вони використовували дві різні архітектури, одна з яких розглядала зображення як випадкові змінні, а пікселі як результати, а друга – навпаки. Обличчя людей пов’язані багатьма способами, але пошук незалежних основних облич може покращити представлення. Просторово локалізовані вектори ознак використовуються для їх статистичної незалежності, що робить їх менш чутливими до закритих частин обличчя. Ще одна відмінність від PCA полягає в

тому, що обчислені вектори в ICA не обов'язково є ортогональними, що робить їх більш гнучкими та кращими для реконструкції вихідних даних. Найпоширеніший підхід на основі статистичних ознак називається прихованими моделями Маркова (HMM). Він побудований на використанні ланцюга Маркова з кінцевою кількістю станів, матриці ймовірності переходу стану, розподілу ймовірності початкового стану та набору функцій щільності ймовірності, пов'язаних з кожним станом. Спочатку зображення скануються в 1D або 2D і витягується набір блоків. Потім риси виділяються, як вони з'являються в природному порядку зверху вниз, і кожній області обличчя призначається стан у HMM. Нарешті, процедура максимального відбору використовується для пошуку найбільш ймовірного збігу.

Аналіз локальних особливостей (LFA) — це біологічно натхненний метод, який використовується для виділення місцевих топографічних особливостей з метою усунення статистичної надмірності. Цей метод подібний до того, як мозок має виявити, які об'єкти знаходяться в полі зору, за допомогою активності рідко розподілених рецепторів.

Зазвичай представлення ознак виконується за допомогою так званих вейвлетів Габора. Кожну функцію можна описати як струмінь Габора, який є набором коефіцієнтів згортки для ядер різної орієнтації та частот у кожному пікселі. Потім ознаки можна класифікувати за допомогою цілісних дискримінантних методів, таких як LDA.

Дослідження [11] показали, що автоматично витягнуті функції в місцях з найбільшими відхиленнями від очікувань були ефективнішими, ніж використання попередньо визначених місць.

1.3.3 Методи зіставлення графів

Використання вейвлетів Габора для захоплення основних візуальних особливостей, таких як очі, ніс і рот, також було представлено разом із структурою під назвою архітектура динамічного зв'язку (DLA). З цього виник інший метод під назвою зіставлення графа еластичної згортки (EBGM), який ще більше узагальнив представлення графа. Віскот та ін. [12] представив груповий

граф як нову структуру даних, яка побудована з невеликого набору зразкових графів зображень.

Зіставлення графіків зазвичай виконується у два послідовних кроки, де перший – це жорстке вирівнювання сітки для врахування глобальних перетворень графіка. По-друге, вузли сітки порівнюються за допомогою функції подібності графіка.

Графіки, як правило, є інваріантними до обертання, тому вони стійкі до змін пози, але недоліком є те, що вони також дуже дорогі з точки зору обчислень. Моделювання форми — це ще одна форма методів, що використовуються в гнучких моделях зовнішнього вигляду (FAM) або активних моделях зовнішнього вигляду (AAM). Ці моделі ітеративно деформуються, щоб відповідати прикладам форм у нових зображеннях за допомогою різних процедур підгонки. 10 варіантів у межах класу класифікуються за допомогою дискримінантного аналізу та будується глобальна безформна модель рівня сірого. Ланітіс та ін. [13] розгорнули повністю автоматичну надійну систему ідентифікації обличчя з використанням гнучких моделей. Розпізнавання на основі компонентів, що використовується, може додатково покращити гнучкі геометричні моделі, використовуючи набір компонентів обличчя, які з’єднані між собою також за допомогою компонентів градації сірого. Ідея полягає в тому, що компоненти можуть моделювати позу голови та інші зміни, просто змінюючи положення всередині моделі. Схему моделі активної зовнішності використовували Кутес та інші [14] з використанням статистичних моделей зовнішнього вигляду. Їхня модель вимагала близького вихідного положення лицьових точок для досягнення надійних і швидких конвергентів. Однак така інформація рідко доступна заздалегідь, і без неї процедура пошуку може зайняти багато часу.

1.3.4 Нейронні методи

У пошуках ще кращого узагальнення класів обличчя також були протестовані нейронні мережі, такі як Probabilistic Decision-Based Neural Network (нейронна мережа на основі ймовірнісних рішень, далі PDBNN) і Evolutionary

Pursuit (еволюційна гонитва, далі EP). Ці типи процедур навчання покращують межі прийняття рішень за допомогою функцій пристосованості.

PDBNN [15] складається з трьох модулів: детектора обличчя, локалізатора очей і розпізнавача обличчя. Він приймає ієрархічну мережеву структуру з нелінійними базовими функціями, де для розпізнавання використовується інформація про інтенсивність ознак і країв.

З іншого боку, EP реалізує характеристики генетичних алгоритмів (ГА) для пошуку простору можливих рішень і визначення оптимального базису. Дані спочатку проектуються в нижчий вимірний простір, подібний до PCA, а потім GA шукають випадкові повороти базисних векторів.

Інша система нейронної мережі називається згорткова нейронна мережа (CNN), яка використовує самоорганізуючу карту (SOM). SOM використовується для квантування зразків зображень у топологічний простір так, щоб подібні об’єкти були поруч один з одним. Це робить процедуру зіставлення інваріантною до невеликих змін у зображеннях.

1.4 Висновки до розділу

Отже, у даному розділі було проведено аналіз методів біометричної ідентифікації для користувачів, досліджено та розглянуто кожний з усіх методів. Створено таблицю з порівнянням методів ідентифікації та їх характеристик відносно таких критеріїв як: переваги, недоліки, ймовірність помилки першого роду, ймовірність помилки другого роду, ефективність методу.

Також було встановлено, що на даний час динамічні методи ідентифікації, які побудовані на основі розпізнавання обличчя завдяки своїй універсальності та зручності в використанні є найбільш перспективними для подальшого дослідження та розвитку. Зокрема, це методи, що аналізують особливості клавіатурного почерку, що особливо актуально в теперішніх умовах, так як майже жодне робоче місце неможливо уявити без персонального комп’ютера.

Таким чином при подальших дослідження було сконцентровано увагу на підвищенні якості ідентифікації за допомогою розпізнавання обличчя користувача з використанням сучасних методів ймовірнісного і статистичного моделювання та нейромереж.

2 МЕТОДИ ТА МОДЕЛІ ДЛЯ ДЕТЕКЦІЇ

2.1 Аналіз методів детекції користувача

У сучасному світі різноманітні системи для розпізнавання облич призначені з метою автоматичної ідентифікації особистості за допомогою відеопотоків. Такі системи виробляють не лише розпізнавання рис облич та образів, з метою перевірки завчасно створених фотоілюстрацій у базах даних. Насамперед винайдені системи для подібних цілей обробляють інформацію за допомогою відеокамери і функції детектору рис облич. Спершу системна функція детектування перевіряє на співпадіння при появі в кадрі персони і фіксує зображення тієї чи іншої особи.

Усі зображення мають бути спочатку зроблені камерою, а потім передані на комп’ютер застосування зору для подальшої обробки. Порівняно із зоровою системою людини камера — це око, а програмне забезпечення для обробки — мозок програми. Приклад того, як людина бачить об’єкт кота, і як програма комп’ютерного зору бачить той самий об'єкт, показано на рис 2.1.

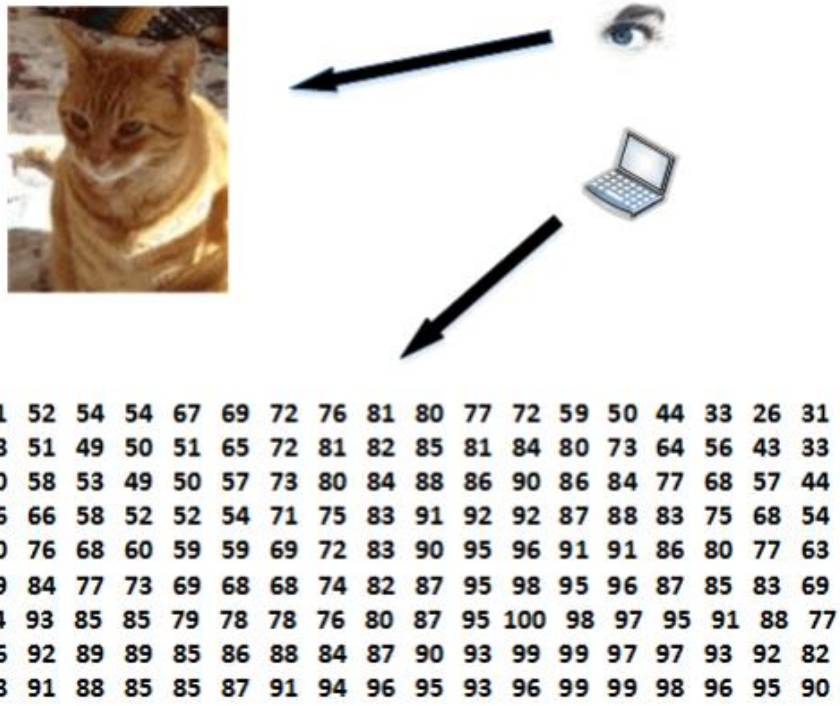


Рисунок 2.1 – Порівняння зору людини та комп’ютера

Людська зорова система без зусиль інтерпретує об’єкт як кішку. У неї немає проблем інтерпретації тонких варіацій напівпрозорості та правильного сегментування об’єкта, як кота та його фона. Людське око і мозок здатні до вилучення детальної інформації із зображення за допомогою існуючого шаблону розпізнавання років досвіду та еволюції.

Крім того, система людського зору вловлює об’єкти у трьох вимірах з такими контекстними властивостями, як глибина, колір, форма та зовнішній вигляд.

Однак усі ці властивості втрачаються, коли камера фіксує зображення та його дані досягають системи комп’ютерного зору. Дані камери представлені у вигляді двовимірної сітки чисел, система має відновити втрачену контекстну інформацію інвертування процесу отримання камерою з невідомої та недостатньої інформації.

Відновлення втрачених контекстних властивостей, візуальна реконструкція зображення та його інтерпретація через недостатню кількість інформації є причиною, що робить процес детекції досить непростим та проблематичним.

Існують наступні методи детекції обличчя [16]:

1) На основі знань:

Метод, заснований на знаннях, залежить від набору правил і ґрунтується на знаннях людини для виявлення облич. Обличчя повинно мати ніс, очі та рот на певній відстані та в певному положенні одне від одного. Великою проблемою цих методів є складність побудови відповідного набору правил. Може бути багато хибних спрацьовувань, якщо правила були надто загальними або надто детальними. Самого цього підходу недостатньо, і він не може знайти багато облич на кількох зображеннях.

2) На основі функцій:

Метод, заснований на ознаках, полягає у визначенні облич шляхом виділення структурних особливостей обличчя. Спочатку він тренується як класифікатор, а потім використовується для розрізнення між лицевими та нелицевими областями. Ідея полягає в тому, щоб подолати межі нашого інстинктивного знання облич. Цей підхід, поділений на кілька етапів, і навіть фотографії з багатьма обличчями має досить високу точність.

3) Відповідність шаблону:

Метод зіставлення шаблонів використовує попередньо визначені або параметризовані шаблони облич для пошуку або виявлення облич за кореляцією між шаблонами та вхідними зображеннями. Обличчя людини можна розділити на очі, контур обличчя, ніс і рот. Крім того, модель обличчя може бути побудована за ребрами, просто використовуючи метод виявлення країв. Цей підхід простий у реалізації, але він недостатній для виявлення обличчя. Однак для вирішення цих проблем були запропоновані шаблони, що деформуються, див. рис 2.2.

Рисунок 2.2 – Приклад роботи методу зіставлення шаблонів

4) На основі зовнішнього вигляду:

Метод на основі зовнішнього вигляду залежить від набору зображень облич делегатів для навчання, щоб знайти моделі облич. Підхід, заснований на зовнішньому вигляді, кращий за інші способи виконання. Загалом метод на основі зовнішнього вигляду покладається на методи статистичного аналізу та

машинного навчання, щоб знайти релевантні характеристики зображень обличчя. Цей метод також використовується для виділення ознак для розпізнавання обличчя.

Модель, заснована на зовнішньому вигляді, далі розділена на наступні підметоди, а саме:

4.1) На основі власних граней:

Алгоритм на основі власних граней, який використовується для розпізнавання облич, і це метод для ефективного представлення облич за допомогою аналізу головних компонентів.

4.2) На основі розподілу:

Алгоритми, такі як PCA та дискримінант Фішера, можна використовувати для визначення підпростору, що представляє візерунки обличчя. Існує навчений класифікатор, який правильно ідентифікує екземпляри цільового класу шаблону з шаблонів фонового зображення.

4.3) Нейронні мережі:

Нейронні мережі успішно вирішують багато проблем виявлення, наприклад виявлення об’єктів, обличчя, емоцій, розпізнавання обличчя тощо.

4.4) Метод опорного вектора:

Метод опорних векторів — це лінійні класифікатори, які максимізують запас між гіперплощиною рішення та прикладами в навчальному наборі.

4.5) Розріджена мережа елементів:

Метод визначає розріджену мережу з двох лінійних одиниць або цільових вузлів; один представляє візерунки обличчя, а інший для шаблонів без обличчя. Характеризується як менш трудомісткий та ефективний.

4.6) Наївний класифікатор Байєса:

Обчислює ймовірність того, що обличчя буде присутнім на зображенні, підрахувавши частоту появи серії візерунка на навчальних зображеннях. Класифікатор фіксує спільну статистику локального зовнішнього вигляду та положення облич.

4.7) Прихована модель Маркова (ПММ):

Станом моделі будуть риси обличчя, які зазвичай описуються як смуги пікселів. ПММ зазвичай використовується разом з іншими методами для створення алгоритмів виявлення.

4.8) Теоретичний підхід до інформації:

Випадкові поля Маркова (MRF) можна використовувати для візерунка обличчя та корельованих ознак. Процес Маркова максимізує розрізнення між класами за допомогою розбіжності Кульбака-Лейблера. Тому цей метод можна використовувати в розпізнаванні обличчя.

4.9) Індуктивне навчання:

Цей підхід використовувався для виявлення облич. Для цього використовуються такі алгоритми, як C4.5 Квінлана [17] або FIND-S Мітчелла [18].

4.10) Гручке порівняння на графах:

Метод заснований на еластичному порівнянні графів, які в свою чергу описують зображення осіб. Особи представляються у вигляді графів зі зваженими вершинами та ребрами [19]. Далі під час розпізнавання один з них (еталонний) – не змінюється, а інший в свою чергу змінюється для найкращого пасування до першого. Графи у таких системах можуть бути як прямокутного типу так і структурою утвореною характерними точками, див. рис 2.3.

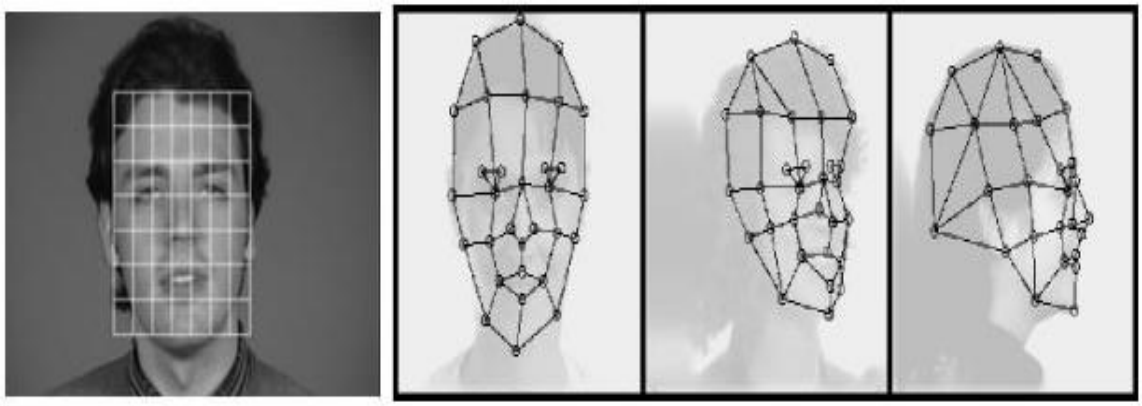


Рисунок 2.3 – Структура графа для розпізнавання осіб

Точність роботи проаналізованих вище методів наведена в наступній таблиці.

Таблиця 4 – Точність роботи методів детекції користувача

Метод детекції	Кількість зображень	Правильний результат розпізнавання
Метод головних компонент [5]	400	79.65%
Компонентий аналіз	400	92.34%
Незалежний аналіз компонентів [6]	100	81.3%
Вейвлет-перетворення [7]	100	80–90%
Модель активної форми [8]	100	78.12–91%
Прихована модель Маркова [9]	200	84%
Метод власних граней [10]	70	92–95%
Метод опорних векторів [11]	200	85–91%
Нейронні мережі	200	93.7%

На рисунку 2.4 наведено блок схему загального процесу детекції користувача.

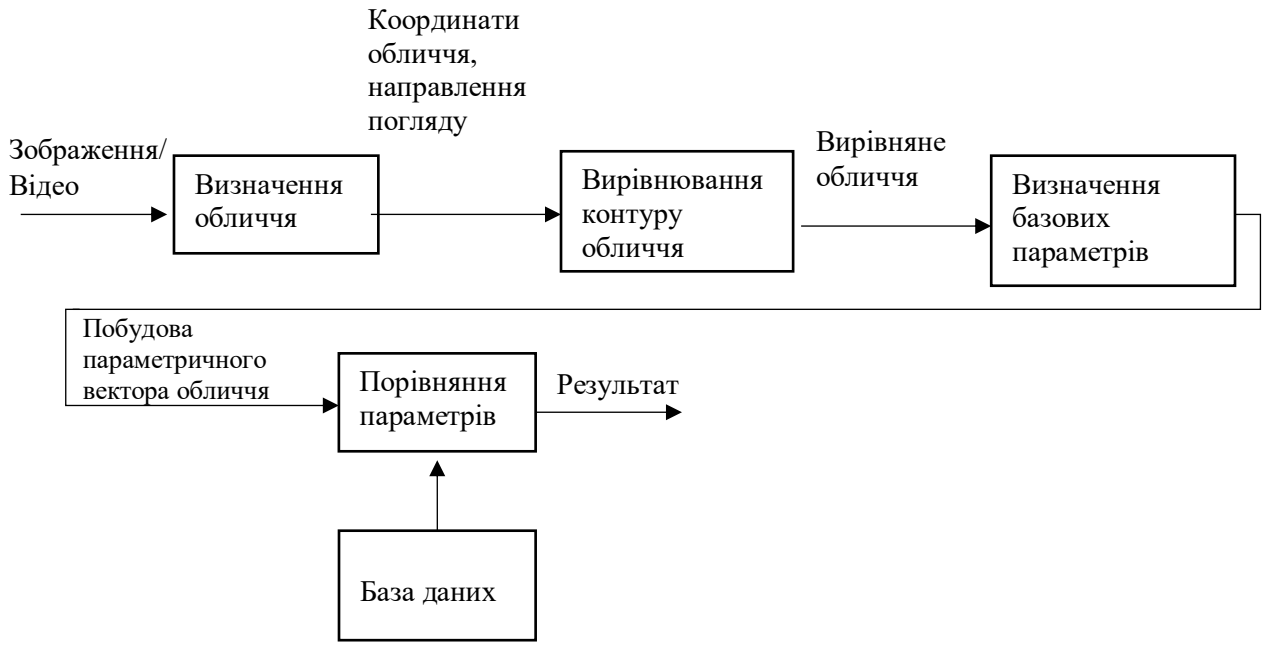


Рисунок 2.4 – Схема роботи процесу детекції

2.2 Принцип роботи алгоритму розпізнавання обличчя

Існує багато методів виявлення облич, за допомогою цих методів ми можемо розпізнати обличчя з більшою точністю. Ці методи мають майже однакову процедуру для виявлення облич, як OpenCV [20], нейронні мережі, Matlab [21] тощо. Проте у всіх них є деякі схожі кроки, які вони використовують для розпізнавання облич, а саме:

– Спочатку зображення імпортується шляхом надання розташування зображення. Потім зображення перетворюється з RGB на градації сірого, оскільки в градаціях сірого легко розпізнати обличчя див. рис. 2.5;

Рисунок 2.5 – Конвертація вхідного зображення на градації сірого

– Після цього використовується маніпуляція зображенням, під час якої за потреби виконується зміна розміру, кадрування, розмивання та підвищення різкості зображень;

– Наступним кроком є сегментація зображення, яка використовується для визначення контурів або сегментації кількох об’єктів на одному зображенні, щоб класифікатор міг швидко виявити об’єкти та обличчя на зображенні;

– Наступним кроком є використання алгоритму Віоли – Джонса, який дещо схожий до ознакам Хаара, для виявлення облич. Цей алгоритм використовується для визначення розташування облич людей у кадрі чи зображенні. Усі людські обличчя мають деякі універсальні властивості

людського обличчя, наприклад область очей темніша за сусідні пікселі, а область носа яскравіша за область очей. Алгоритм, подібний до Хаара, також використовується для виділення ознак або виділення ознак для об’єкта на зображенні за допомогою визначення країв, виявлення ліній, виявлення центру для виявлення очей, носа, рота тощо на зображенні, див. рис. 2.6;

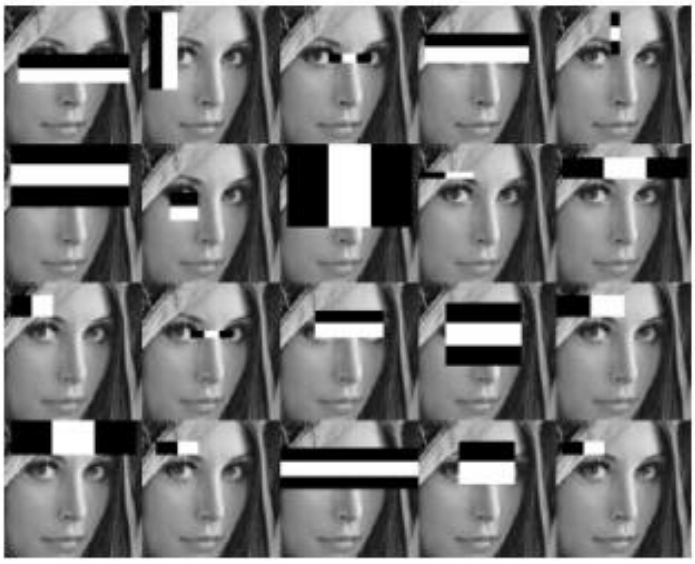


Рисунок 2.6 – Особливості лиця за ознаками Хаара

– Фінальним кроком є визначенння координати x, y, w, h, які утворюють прямокутну рамку на зображенні, щоб показати розташування обличчя або, можна сказати, щоб показати область інтересу на зображенні. Після цього він може створити прямокутну рамку в зоні інтересу, де він виявляє обличчя. Існує також багато інших методів виявлення, які використовуються разом для виявлення, наприклад посмішки, очей, моргання тощо, див. рис. 2.7;

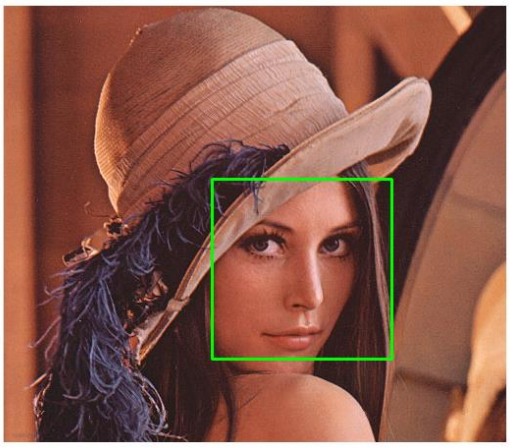


Рисунок 2.7 – Приклад виявленого обличчя на зображенні

2.3 Нейромережевий підхід до задачі детекції

На даний час найбільш поширеними нейромережевими моделями детекції є наступні:

– модель пропозиції областей (R-CNN, FAST R-CNN, FASTER R-CNN);
– модель Single Shot Detection;
– модель Yolo (You Only Look Once);
– модель RefineDet;
– модель Retina-Net;
– модель деформованих згорткових мереж (CNN);

Далі розглянемо кожну із них більш детально:

– модель пропозиції областей - ця модель ідентифікує різні об’єкти присутні на зображенні, для того щоб зменшити час обчислень він використовує інноваційний процес під назвою "Selective Search"(вибірковий пошук) [22]. У цьому процесі сегментація зображення спочатку виконується на зображенні, яке розділяє зображення на різні сегменти шляхом групування суміжних пікселів на основі кольору та текстури, після сегментації зображення навколо сегментованого створюються рамки різного розміру об'єктів. Ці рамки містять об’єкти. Приклад процесу вибіркового пошуку показаний на рисунку 2.8. На рисунку 2.9 наведено алгоритм роботи R-CNN моделі.

Рисунок 2.8 – Приклад вибіркового пошуку на зображенні

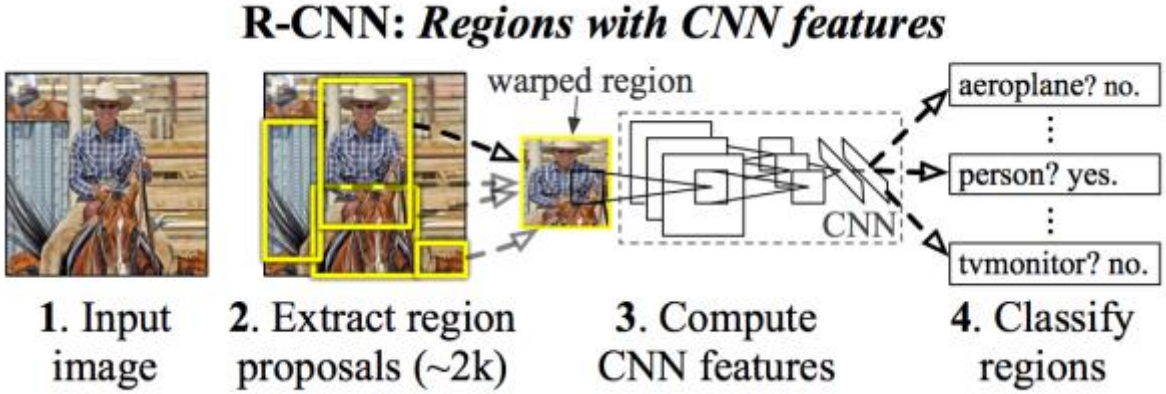


Рисунок 2.9 – Алгоритм роботи R-CNN моделі

– модель Single Shot Detection – це модель одноразового детектора (SSD) була вперше представлена Вей Лю та ін. у статті "SSD: Single Shot MultiBox Detector" [23]. "Один постріл" означає, що виявлення об’єкта та завдання класифікації виконуються за один прохід мережі. Запропонована модель є швидкою і має хорошу точність. Основна ідея SSD полягає в передбаченні об’єктів з балами точності за допомогою малих згорткових фільтрів. Архітектура моделі SSD показана на малюнку 2.10.

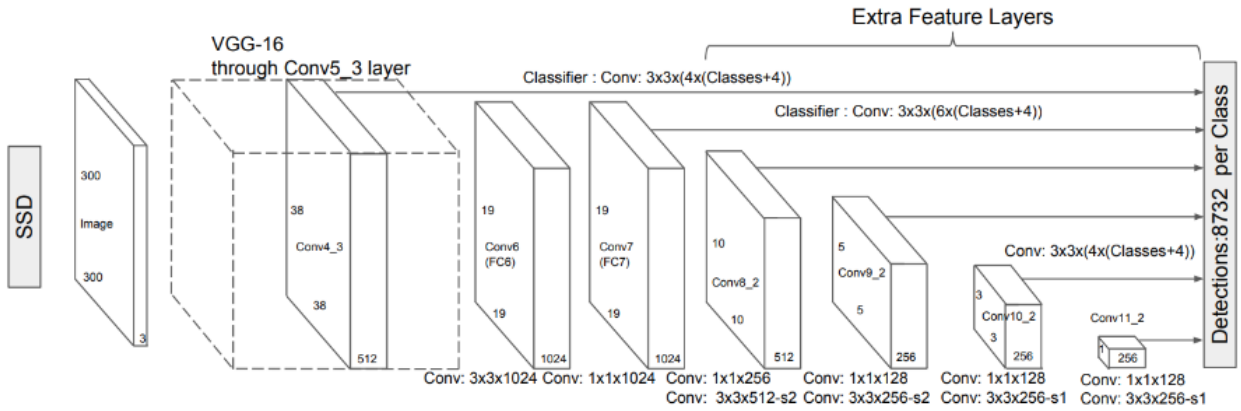


Рисунок 2.10 – Архітектура моделі SSD

– модель YOLO – це алгоритм виявлення об'єктів, який використовує регресійні методи. Як випливає з назви, оцінка зображення виконується за один прохід, замість запуску зображення кілька разів. Була розроблена Джозефом та ін. [24]. Модель YOLO має наскрізний каркас, що робить її надзвичайно швидкою. Базова мережа працює зі швидкістю 45 кадрів за секунду (кадрів за секунду), але може досягати до 150 кадрів за секунду, що дає можливість виявляти об’єкти в реальному часі. Ця модель має затримку менше 25 мілісекунд під час обробки відео в реальному часі. Ще однією її перевагою перед іншими моделями є те, що замість використання повільніших методів, таких як ковзаюче вікно та методи на основі пропозицій, YOLO використовує все зображення один раз для навчання, а також для тестування. Приклад роботи цієї моделі наведений на рисунку 2.11.

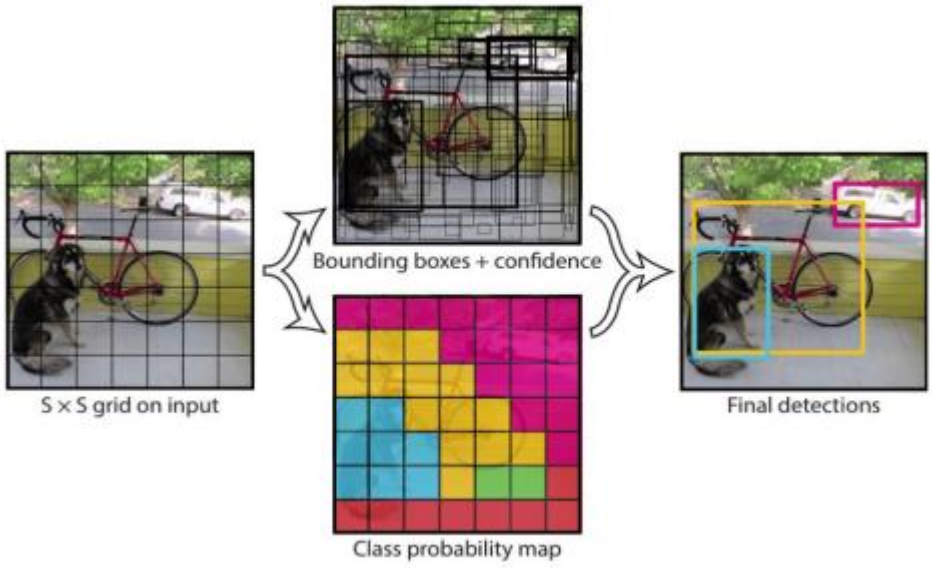


Рисунок 2.11 – Приклад роботи моделі YOLO

– модель RefineDet - принцип роботи цієї моделі полягає в тому що, для того щоб отримати остаточний результат, RefineDet [25] генерує заздалегідь визначену кількість обмежувальних прямокутників і балів, що вказує на існування різних типів елементів у цих вікнах, після чого виконується немаксимальне придушення (NMS). Модуль уточнення прив'язки (ARM) і модуль виявлення об'єктів (ODM) — це два взаємопов'язані компоненти, які загалом і складають RefineDet (ODM). Архітектура цієї моделі наведена на рисунку 2.12.

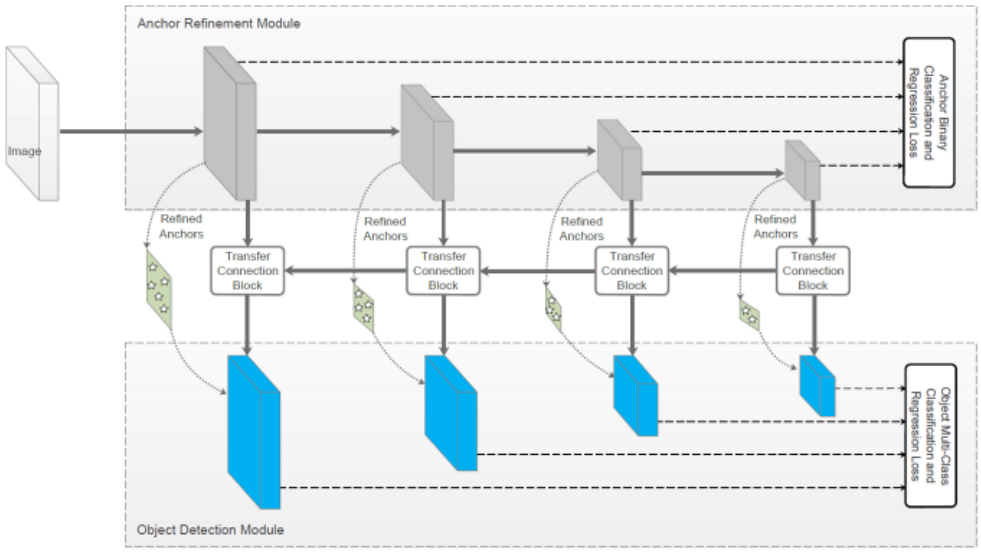


Рисунок 2.12 – Архітектура моделі RefineDet

– модель Retina-Net – архітектура цієї моделі [26] складається з 4 основних частин, а саме (див. рис. 2.13):

1) шлях «знизу вгору» — магістральна мережа (наприклад, ResNet), яка обчислює карти функцій у різних масштабах, незалежно від розміру вхідного зображення чи магістралі.
2) шлях «зверху вниз» і бічні зв'язки. Шлях «зверху вниз» підвищує дискретизацію просторово більш грубих карт характеристик із вищих рівнів піраміди, а бічні зв'язки об'єднують шари «зверху вниз» і «знизу вгору» однакового просторового розміру.

3) класифікаційна підмережа – вона передбачає ймовірність присутності об’єкта в кожному просторовому місці для кожного блоку прив’язки та класу об’єктів.
4) підмережа регресії – регресує зсув для обмежувальних рамок від опорних рамок для кожного наземного об’єкта.

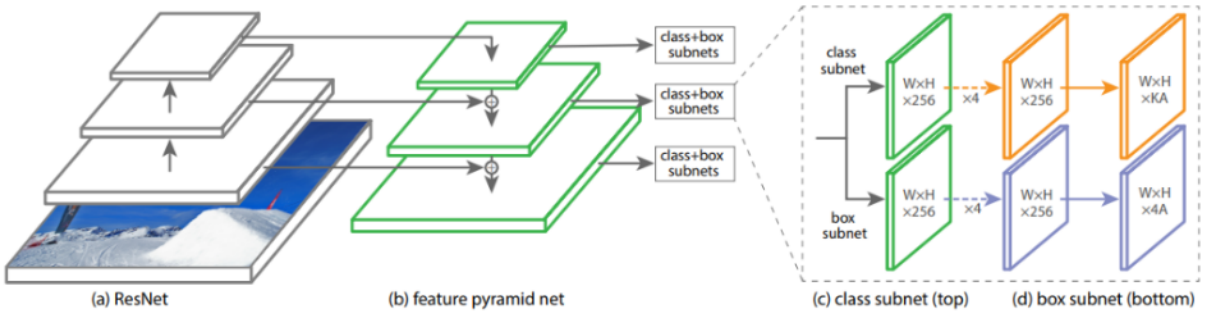


Рисунок 2.13 – Архітектура моделі Retina-Net

– модель CNN - 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 [27]. 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 див. рис. 2.14;

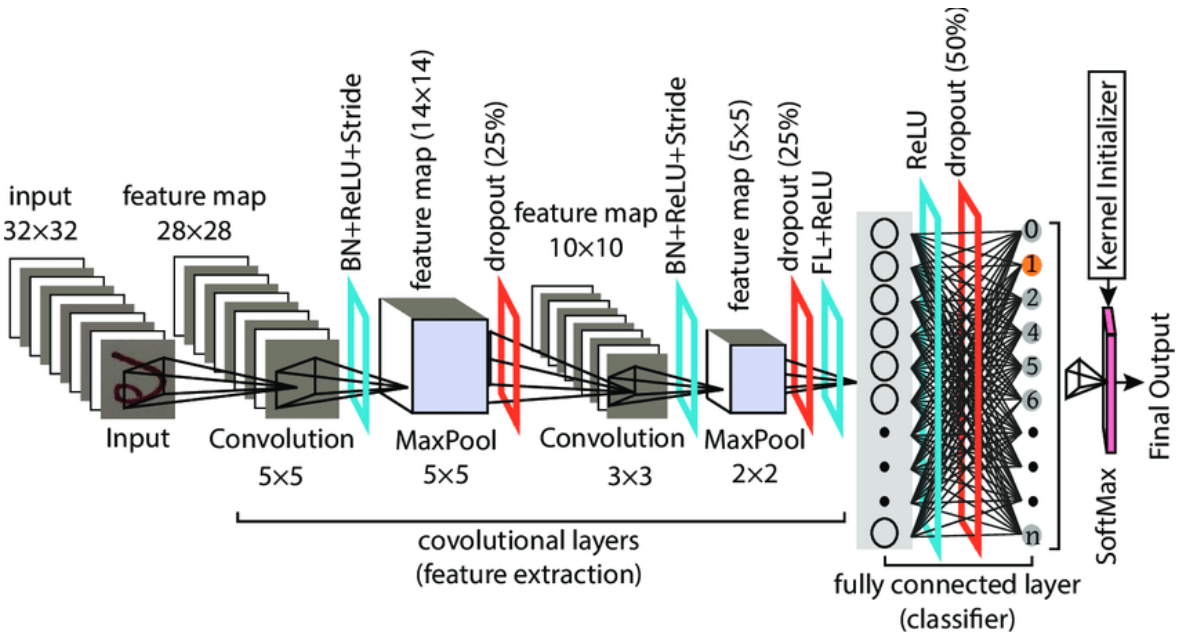


Рисунок 2.14 – Архітектура моделі CNN

Враховуючи наведені вище перелічені характеристики моделей із використанням нейронних мереж, було визначено, що детекція 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.

2.4 Формування матриці вхідних параметрів

Вхідним параметром, для нейромережі, яка використовується для ідентифікації користувача за допомогою розпізнавання його обличчя є зображення, проте перед тим як перетворити його в матрицю, це зображення потрібно попередньо підготувати, а саме:

– зменшити його розмірність до необхідної;
– обрізати його в формі квадрату;
– нормалізувати освітлення;
– провести нормалізацію зображення, щоб mean (середнє значення) було нулем, а середньо квадратичне відхилення було одиницею;

Приклад нормального розподілу наведено на рисунку 2.15.

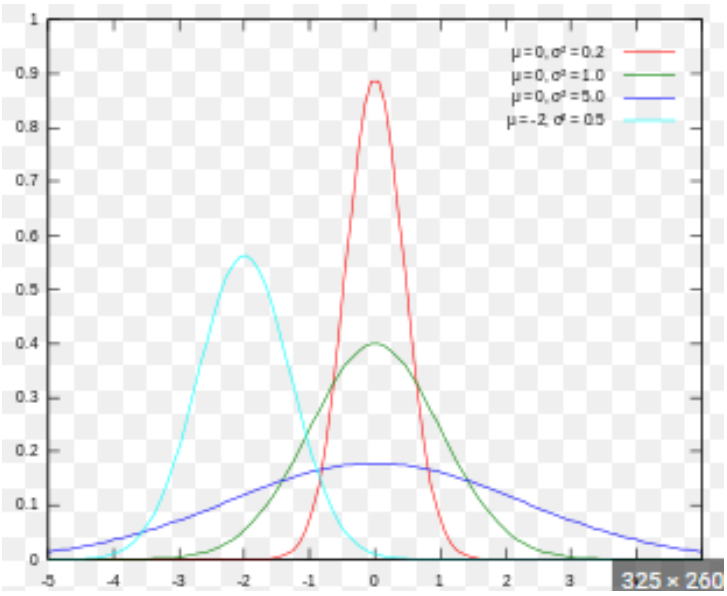


Рисунок 2.15 – Приклад нормального розподілу

Попередня підготовка зображення, необхідна для правильної та точної роботи системи, оскільки дозволяє знизити рівень шуму на зображенні, та покращити її швидкість роботи, завдяки зменшенню розмірності, див. рис. 2.16.

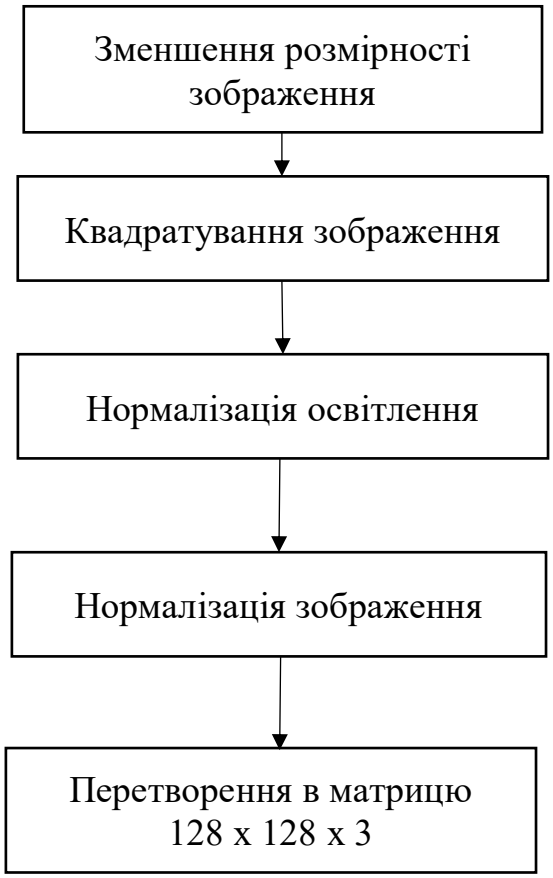


Рисунок 2.16 – Схема роботи попередньої обробки зображення

В результаті перетворень на вхід буде отримано трьох вимірну матрицю, розмірності 128 x 128 x 3, в якій перші два виміри будуть відповідають за координати x та y, а останній за колір зображення.

2.5 Побудова моделі для детекції обличчя користувача за допомогою нейромережі

З урахуванням виразів наведених вище можна запропонувати структуру моделі, яка використовується для ідентифікації користувача за допомогою розпізнавання його обличчя, та яку загалом можна зообразити за допомогою трьох частин:

– input image;

– face detection;

– face recognition;

Вигляд моделі наведений на рисунку 2.17.

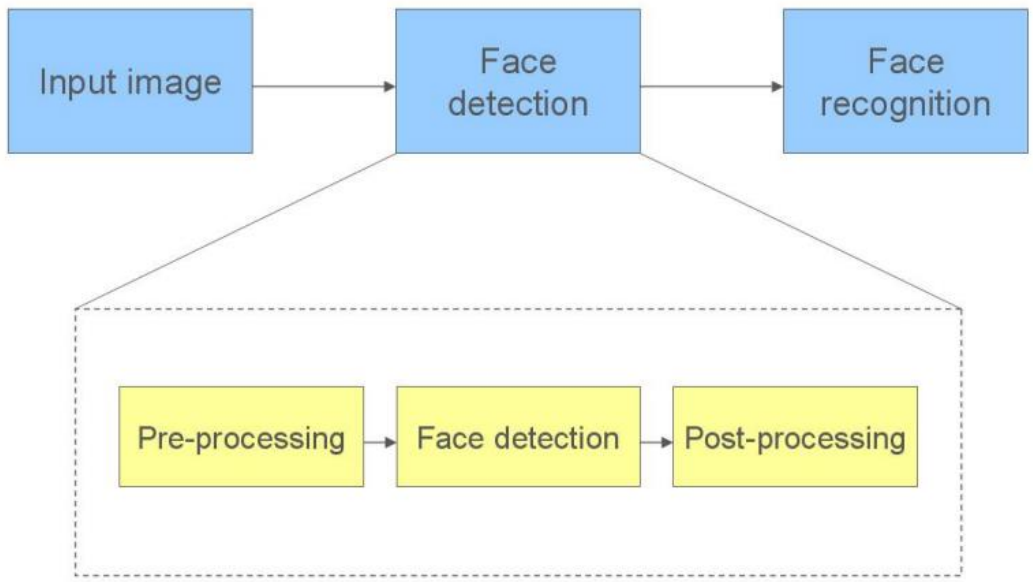


Рисунок 2.17 – Загальний вигляд моделі ідентифікації обличчя користувача

Розглянемо більш детально модуль та модель, яка відповідає саме за детекцію обличчя користувача.

Для вирішення задачі ідентифікації обличчя користувача було створену нейронну мережу на основі моделі BlazeFace [28], яка є легким і високопродуктивним рішенням, з підтримкою мобільного GPU та працює зі швидкістю 200-1000+ FPS на флагманських пристроях.

Ця надвисока продуктивність у реальному часі дає змогу застосовувати його до будь-якого конвеєра доповненої реальності, який потребує точної цікавої області обличчя як вхідних даних для конкретних моделей завдань, таких як 2D/3D оцінка ключових точок обличчя або геометрії, рис обличчя або класифікації виразів, а також сегментація області обличчя. Ця модель, має певні схожі риси з моделлю MobileNetV1/V2, але відмінну від неї, схему прив’язки для графічного процесора, модифіковану з Single Shot MultiBox Detector (SSD), і покращену стратегію вирішення зв’язків, альтернативу немаксимальному придушенню.

Окрім передбачення прямокутників обличчя, вирівняних за віссю, розроблена модель створює 6 координат ключових точок обличчя (для центрів очей, вушних раковин, центру рота та кінчика носа), які дозволяють оцінити поворот обличчя (кут повороту). Це дає змогу передавати повернутий прямокутник обличчя на наступні етапи конвеєра обробки відео, пов’язані з конкретними завданнями, зменшуючи вимогу значної інваріантності переміщення та обертання на наступних етапах обробки.

Архітектура моделі побудована навколо чотирьох важливих міркувань дизайну, розглянутих нижче.

– збільшення розмірів рецептивного поля - у той час як більшість сучасних архітектур згорткових нейронних мереж, включаючи обидві версії MobileNet [29], мають тенденцію віддавати перевагу ядрам згортки 3 × 3 всюди вздовж графа моделі, ми зауважимо, що в обчисленнях згортки, що розділяються по глибині, переважають їх точкові частини. На вхідному тензорі s × s × c згортка

k × k включає операції множення-додавання s^2ck^2, тоді як наступна згортка 1 × 1 у d вихідних каналів складається з s^2cd^2 таких операцій із коефіцієнтом d/k^2 глибинної частини. На практиці, наприклад, реалізація Metal Performance Shaders, 3×3 згортка по глибині в 16-бітній арифметиці з плаваючою комою займає 0,07 мс для тензора 56 × 56 × 128, тоді як наступна згортка 1 × 1 від 128 до 128 каналів є на 4,3 × повільнішою на 0,3 мс (це не настільки суттєво, як чиста арифметика різниця в кількості операцій через постійні витрати та коефіцієнти доступу до пам'яті).

– Це спостереження означає, що збільшення розміру ядра частини по глибині є відносно дешевим. Ми використовуємо ядра 5×5 у вузьких місцях архітектури моделі, обмінюючи збільшення розміру ядра на зменшення загальної кількості таких вузьких місць, необхідних для досягнення певного розміру сприйнятливого поля (рис. 2.18). Вузьке місце MobileNetV2 містить подальше розширення із збільшенням глибини та зменшення глибини проекції поточкових згорток, розділених нелінійністю.

– Щоб пристосуватися до меншої кількості каналів у проміжних тензорах, ці етапи мінялись місцями, щоб залишкові зв'язки в вузьких місцях працювали в «розширеному» (збільшеному) дозволі каналу.

– Нарешті, низькі накладні витрати глибинної згортки дозволяють ввести ще один такий шар між цими двома поточковими згортками, ще більше прискорюючи прогресування розміру рецептивного поля. Це формує суть подвійного BlazeBlock, який використовується як вузьке місце вибору для вищих рівнів абстракції BlazeFace (див. рис 2.18, та рис. 2.19);

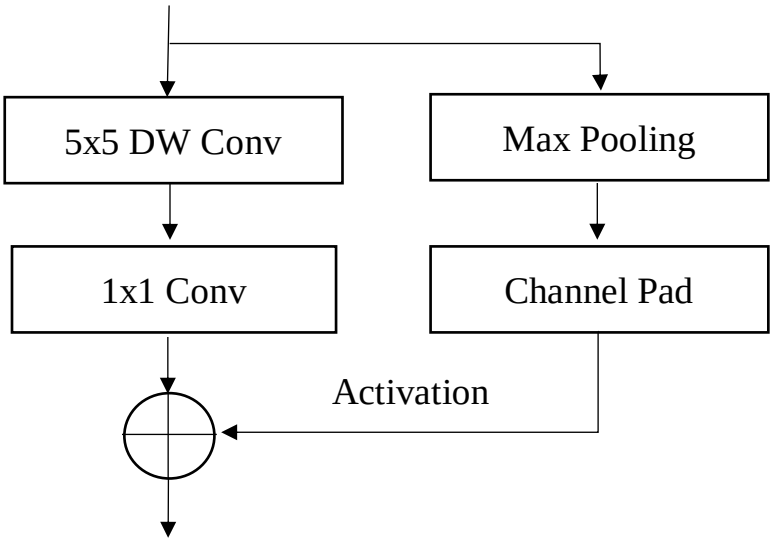


Рисунок 2.18 – Структура Blaze блоку

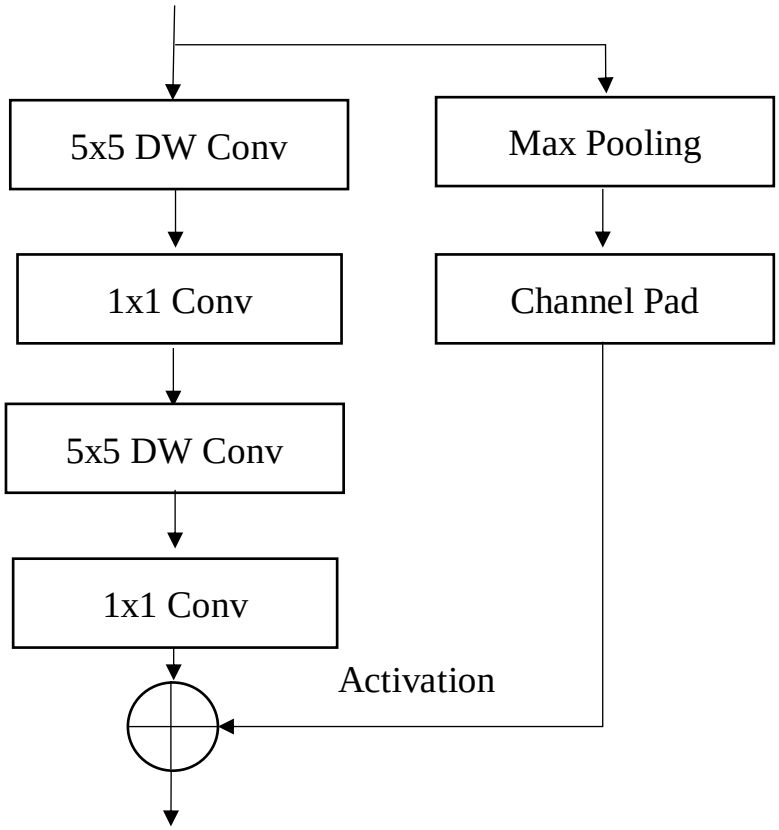


Рисунок 2.19 – Структура подвійного Blaze блоку

– вилучення ознак - для конкретного прикладу ми зосередимося на екстракторі ознак для моделі з фронтальною камерою. Він повинен враховувати менший діапазон масштабів об’єктів і, отже, має менші обчислювальні вимоги.

Екстрактор приймає RGB-вхід 128 × 128 пікселів і складається з 2D-згортки, за якою слідують 5 одиночних Blaze блоків і 6 подвійних Blaze блоків. Найвища глибина тензора (роздільна здатність каналу) становить 96, а найнижча просторова роздільна здатність – 8×8 (на відміну від SSD, який знижує роздільну здатність аж до 1×1);

– схема прив'язки - моделі виявлення об'єктів, подібні до SSD, покладаються на попередньо визначені базові обмежувальні прямокутники фіксованого розміру, які називаються попередніми, або якорями в термінології Faster-R-CNN [30]. Набір параметрів регресії таких як зміщення центру та коригування розмірів, передбачено для кожного прив'язки. Вони використовуються для коригування попередньо визначеної позиції прив'язки в щільно обмежувальний прямокутник. Загальною практикою є визначення прив'язок на кількох рівнях роздільної здатності відповідно до діапазонів масштабу об'єкта. Агресивне зменшення дискретизації також є засобом оптимізації обчислювальних ресурсів. Типова модель SSD використовує передбачення розмірів карти функцій 1×1, 2×2, 4×4, 8×8 і 16×16. Однак успіх архітектури пірамідної мережі об'єднання (PPN) означає, що додаткові обчислення можуть бути зайвими після досягнення певної роздільної здатності карти функцій. Ключовою властивістю GPU на відміну від обчислень CPU є помітна фіксована вартість диспетчеризації обчислень певного рівня, яка стає відносно значною для глибоких рівнів із низькою роздільною здатністю, властивих популярним адаптованим до CPU архітектурам. Як приклад, в одному експерименті було виявлено, що з 4,9 мс часу висновку MobileNetV1 лише 3,9 мс було витрачено на фактичне обчислення шейдера GPU. Беручи це до уваги, було прийнято альтернативну схему прив'язки, яка зупиняється на розмірах карти функцій 8 × 8 без подальшого зменшення дискретизації. Було замінено 2 прив'язки на піксель у кожній із роздільних здатностей 8×8, 4×4 і 2×2 на 6 прив'язок у 8×8. Через обмежену дисперсію пропорцій людського обличчя обмеження прив'язок співвідношення сторін 1:1 було визнано достатнім для точного визначення обличчя, див. рис. 2.20;

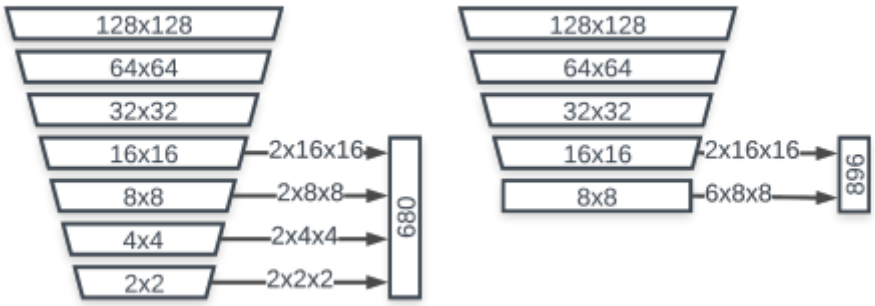


Рисунок 2.20 – Порівняння роботи прив’язки SSD та Blazeface

– подальша обробка - оскільки наш екстрактор функцій не зменшує роздільну здатність нижче 8 × 8, кількість прив’язок, що перекривають даний об’єкт, значно збільшується зі збільшенням розміру об’єкта. У типовому сценарії немаксимального придушення лише один із прив’язок «перемагає» і використовується як кінцевий результат алгоритму. Коли така модель застосовується до наступних відеокадрів, прогнози, як правило, коливаються між різними якорями та демонструють часове тремтіння (шум, який відчуває людина). Щоб мінімізувати це явище, ми замінюємо алгоритм придушення стратегією змішування, яка оцінює параметри регресії обмежувальної рамки як зважене середнє між передбаченнями, що збігаються. Це практично не вимагає додаткових витрат на вихідний алгоритм NMS. Для нашого завдання виявлення обличчя це налаштування призвело до збільшення точності на 10%. Ми кількісно визначаємо кількість тремтіння, передаючи в мережу кілька трохи зміщених версій одного вхідного зображення та спостерігаючи, як це впливає на результати моделі (з урахуванням трансляції). Після описаної модифікації стратегії роздільної здатності зв’язків метрика тремтіння, визначена як середньоквадратична різниця між прогнозами для початкового та зміщеного вхідних даних, знизилася на 40% для нашого набору даних фронтальної камери.

Запропонована модель, яка працює на повному зображенні чи відеокадрі, може служити першим кроком практично будь-якої програми комп’ютерного зору, пов’язаної з обличчям, наприклад, 2D/3D-телескопічних ключових точок

обличчя, оцінки контурів або геометрії поверхні, рис обличчя або класифікації виразів, а також сегментація області обличчя. Подальше завдання в конвеєрі комп'ютерного зору, таким чином, може бути визначено в термінах правильного кадрування обличчя. У поєднанні з декількома оцінками ключових точок обличчя, це кадрування також можна обертати, щоб обличчя всередині було центроване, нормалізовано в масштабі та мало кут повороту, близький до нуля. Це усуває вимогу значної інваріантності щодо трансляції та обертання з моделі для конкретного завдання, дозволяючи краще розподіляти обчислювальні ресурси, результат наведений на рисунку 2.21.

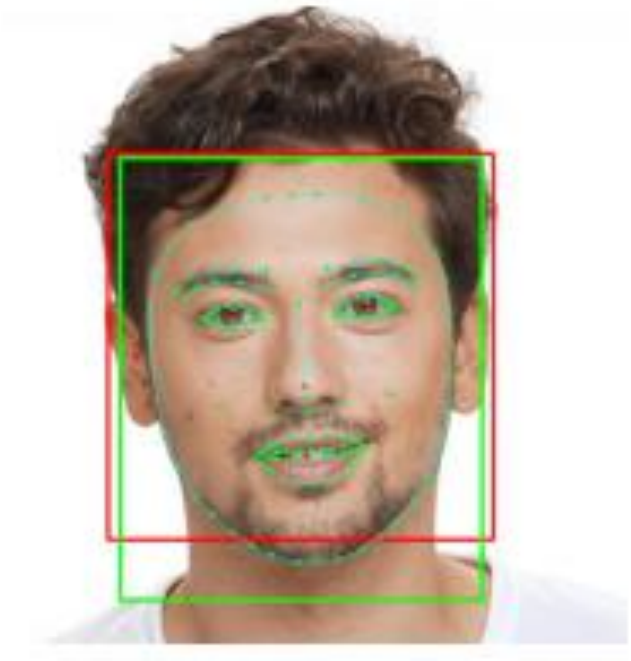


Рисунок 2.21 – Результат роботи моделі

На рисунку показано, як результат роботи моделі, тобто передбачуваний обмежувальний прямокутник і 6 ключових точок обличчя (червоного кольору). Детальні ключові точки дають точнішу оцінку, яку можна повторно використовувати для відстеження в наступному кадрі без запуску детектора обличчя. Щоб виявити помилки цієї стратегії економії обчислень, контурна модель також може визначити, чи дійсно обличчя присутнє та достатньо вирівняно в наданій прямокутній кадрі. Щоразу, коли ця умова порушується, детектор обличчя знову запускається на всьому кадрі відео.

2.6 Висновки до розділу

Отже, у даному розділі було проаналізовано основні методи детекції, її види та категорії. Було досліджено регіональні методи детекції та методи засновані на регресії, досліджено їх переваги та недоліки, було проаналізовано їх техніко економічне обґрунтування. Досліджено точність основних методів детекції в безперервному режимі. Проаналізовано методи детекції користувача з використанням нейронних мереж та наведено причини використання в даній роботі. Описано загальний алгоритм роботи системи детекції та проаналізовано різні види його реалізації. Аргументовано використання всіх запропонованих методів та засобів для детекції користувача.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ДЕТЕКЦІЇ КОРИСТУВАЧА

3.1 Розробка модулю для детекції користувача

Загальна архітектура модулю для детекції користувача виглядає наступним чином:

Таблиця 1 – Архітектура роботи моделі для детекції обличчя

Layer/block	Input size	Conv. kernel sizes
Convolution	128×128×3	5×5×3×24 (stride 2)
Single BlazeBlock	64×64×24	5×5×24×1 1×1×24×24
Single BlazeBlock	64×64×24	5×5×24×1 1×1×24×24
Single BlazeBlock	64×64×24	5×5×24×1 1×1×24×48
Single BlazeBlock	32×32×48	5×5×48×1 1×1×48×48
Single BlazeBlock	32×32×48	5×5×48×1 1×1×48×48
Double BlazeBlock	32×32×48	5×5×48×1 1×1×48×24 5×5×24×1 1×1×24×96
Double BlazeBlock	16×16×96	5×5×96×1 1×1×96×24 5×5×24×1 1×1×24×96
Double BlazeBlock	16×16×96	5×5×96×1 1×1×96×24 5×5×24×1 1×1×24×96
Double BlazeBlock	16×16×96	5×5×96×1 1×1×96×24 5×5×24×1 1×1×24×96
Double BlazeBlock	8×8×96	5×5×96×1 1×1×96×24 5×5×24×1 1×1×24×96
Double BlazeBlock	8×8×96	5×5×96×1 1×1×96×24 5×5×24×1 1×1×24×96

Як бачимо з архітектури наведеної вище, розроблена модель для роботи використовує конволюції (згортки), на кожному блоці в моделі відбувається конволюція вхідної матриці, яка дозволяє витягувати контори на перших кроках, а далі робити картинку більш чіткою, та розпізнавати певні риси.

Згорткова нейронна мережа (ConvNet/CNN) [31] — це алгоритм глибокого навчання, який може сприймати вхідне зображення, призначати важливість (вагові значення та зміщення) різним аспектам/об’єктам на зображенні та мати можливість відрізнити один від іншого. Попередня обробка, необхідна в ConvNet, набагато менша порівняно з іншими алгоритмами класифікації. У той час як у примітивних методах фільтри розробляються вручну, після достатнього навчання, ConvNets мають можливість вивчати ці фільтри/характеристики.

Архітектура ConvNet аналогічна структурі підключення нейронів у людському мозку та була натхненна організацією зорової кори. Окремі нейрони реагують на стимули лише в обмеженій області поля зору, відомої як рецептивне поле. Набір таких полів перекривається, щоб охопити всю візуальну область.

ConvNet може успішно фіксувати просторові та часові залежності в зображенні за допомогою застосування відповідних фільтрів. Архітектура забезпечує кращу адаптацію до набору даних зображення завдяки зменшенню кількості залучених параметрів і можливості повторного використання вагових коефіцієнтів. Іншими словами, мережу можна навчити краще розуміти складність зображення.

На наступному рисунку ми маємо зображення RGB, яке розділене трьома кольоровими площинами — червоною, зеленою та синьою. Існує кілька таких колірних просторів, у яких існують зображення — відтінки сірого, RGB, HSV, CMYK тощо (див. рис. 3.1).

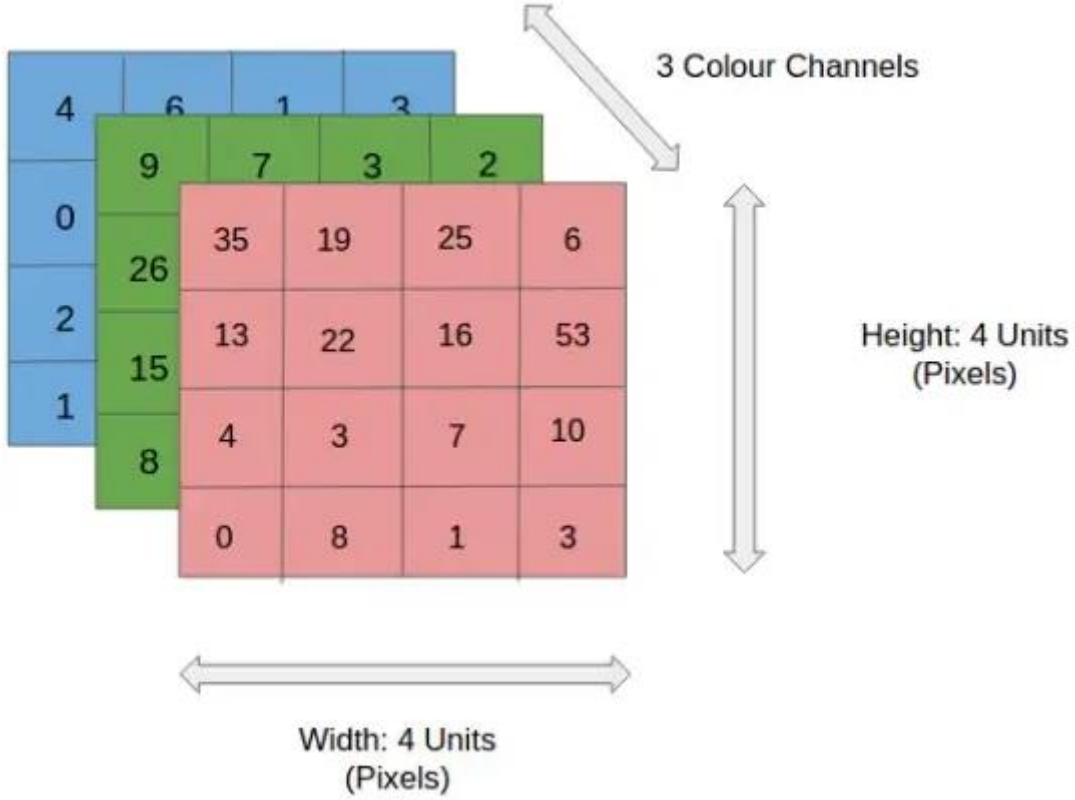


Рисунок 3.1 – Вигляд зображення в 3-д форматі

Можна уявити, наскільки обчислювально інтенсивними будуть речі, коли зображення досягнуть розміру, скажімо, 8K (7680 × 4320). Роль ConvNet полягає в тому, щоб зменшити зображення до форми, яку легше обробляти, без втрати функцій, які є критично важливими для отримання хорошого прогнозу.

Цей фактор є дуже важливим, і був врахований під час розробки архітектури, що дозволяє їй масштабуватись до масивних наборів даних. Приклад розпізнавання зображення наведений на рисунку 3.2.

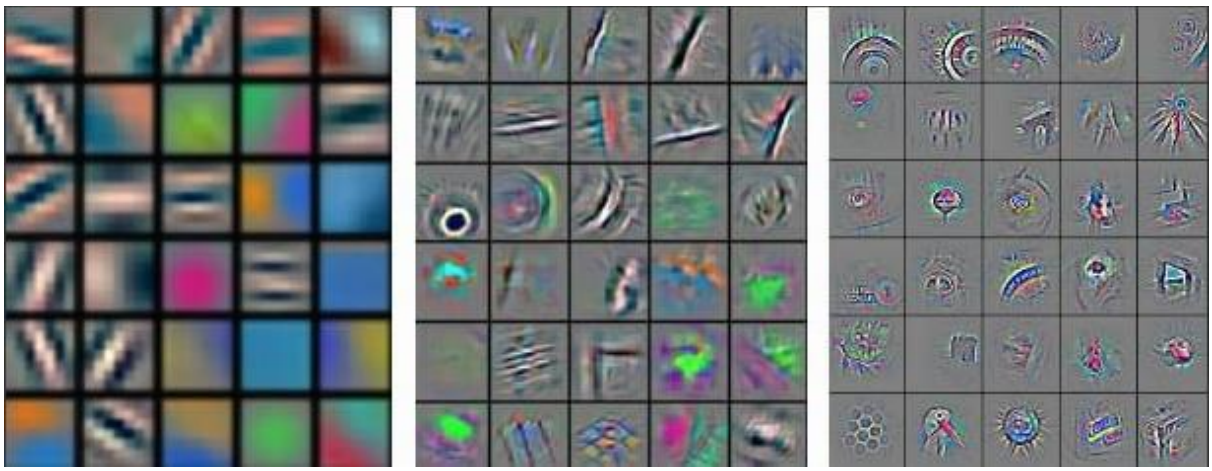


Рисунок 3.2 – Приклад розпізнавання зображення за допомогою CNN мережі

Подібно до згорткового рівня, рівень об’єднання відповідає за зменшення просторового розміру згорнутого об’єкта. Це робиться для зменшення обчислювальної потужності, необхідної для обробки даних, шляхом зменшення розмірності. Крім того, це корисно для виділення домінуючих характеристик, які є обертальними та позиційними інваріантними, таким чином підтримуючи процес ефективного навчання моделі.

Існує два типи об’єднання: максимальне об’єднання та середнє об’єднання. Max Pooling повертає максимальне значення з частини зображення, охопленої ядром. З іншого боку, Average Pooling повертає середнє значення всіх значень із частини зображення, охопленої ядром.

Max Pooling також працює як шумопоглинач. Він повністю відкидає шумні активації, а також виконує усунення шумів разом із зменшенням розмірності. З іншого боку, Average Pooling просто виконує зменшення розмірності як механізм придушення шуму. Саме під час розробки моделі було використано max pooling.

Задля більшої ефективності моделі було використано поглиблена згортку - це тип згортки, де застосовується один згортковий фільтр для кожного вхідного каналу. У звичайній двовимірній згортці, що виконується на кількох вхідних каналах, фільтр є таким же глибоким, як і вхід, і дозволяє нам вільно міксувати канали для створення кожного елемента на виході.

Реалізація поглибленої згортки були виконана наступним чином:

– вхід і фільтр на канали були розділені;
– кожен вхід згортається за допомогою відповідного фільтра;
– згорнуті виходи складаються разом;

Розроблений модуль для детекції складається за наступних класів, кожен з яких відповідає за певну частину роботи системи. Основним класом є клас MediaPipeFaceDetector, який власне і виконує детекцію обличчя за допомогою наступного коду:

```
export class MediaPipeFaceDetectorTfjs implements FaceDetector
  private readonly imageToTensorConfig: ImageToTensorConfig;
  private readonly tensorsToDetectionConfig:
TensorsToDetectionsConfig;
  private readonly anchors: Rect[];
  private readonly anchorTensor: AnchorTensor;
  constructor(
      detectorModelType: 'short'|'full',
      private readonly detectorModel: tfconv.GraphModel,
      private readonly maxFaces: number) {
    if (detectorModelType === 'full') {
      this.imageToTensorConfig =
constants.FULL_RANGE_IMAGE_TO_TENSOR_CONFIG;
      this.tensorsToDetectionConfig =
          constants.FULL_RANGE_TENSORS_TO_DETECTION_CONFIG;
      this.anchors =
createSsdAnchors(constants.FULL_RANGE_DETECTOR_ANCHOR_CONFIG);
    }
```

Проте перед тим почати використовувати цей клас, потрібно проініціалізувати систему, оскільки у наведеному коді вище видно що в конструктор потрібно передати певні конфігурацію для створення його екземпляру.

Ця конфігурація складається з наступних параметрів:

– runtime - в нашій моделі, це ‘tfjs’;

– maxFaces - максимальна кількість облич, які буде виявлено моделлю. Потрібно обов’язково встановити для цього параметра значення очікуваної максимальної кількість граней, інакше модель продовжить пошук відсутніх граней, що може сповільнити продуктивність;

– modelType - необов’язковий параметр. Можливі значення: 'short' | 'full'. За замовченням встановлено значення 'short'. Модель короткого діапазону, яка найкраще підходить для облич у межах 2 метрів від камери, тоді як модель повного діапазону найкраще підходить для облич у радіусі 5 метрів. Для опції повного діапазону використовується розріджена модель для покращеної швидкості висновку;

Приклад коду для ініціалізації системи наведений нижче:

```
const model = faceDetection.SupportedModels.MediaPipeFaceDetector;
const detectorConfig = {
runtime: ‘tfjs’,
     maxFaces: 1,
modelType: ‘short’,
}
const detector = await faceDetection.createDetector(model,
detectorConfig);
```

Після чого вже можна використовувати детектор обличчя, передаючи попередньо оброблене та нормалізоване зображення. Приклад коду використання наведено нижче:

```
const useGetPicture = ()=> {
  const context = canvas.getContext("2d");
  if (width && height) {
    canvas.width = width;
    canvas.height = height;
    context.drawImage(video, 0, 0, width, height);

    const data = canvas.toDataURL("image/png");
    photo.setAttribute("src", data);
  } else {
    clearphoto();
  }
}
let image = useGetPicture();
const {descaleImage, cropImage, adjustLighting, normalizeImage} =
useImageUtils();
const faces = await detector.estimateFaces(image);
```

Функція estimateFaces в свою чергу поверне масив, у якому вигляді об’єкта буде представлено виявлене обличчя із заданого зображення. У випадку якщо модель не змогла виявити обличчя, цей масив буде порожнім. Приклад результату роботи функції наведений нижче:

```
[
  {
    box: {
```

```
      xMin: 314.6476503248806,
      xMax: 602.5146672117332,
      yMin: 119.32291152347956,
      yMax: 377.035215984403,
      width: 199.86424906415258,
      height: 251.89222233073949,
    },
    keypoints: [
      {x: 476.544134219890, y: 273.813333261923, name: "rightEye"},
      {x: 403.52112753142476, y: 254.4, "leftEye },
      ...
    ],
  }
]
```

Далі результати роботи системи, а саме координати рамки обличчя в просторі пікселів зображення, де xMin, xMax позначають межі координати x, yMin, yMax позначають межі координати y, а ширина, висота є розмірами обмежувальної рамки, разом з шістьма ключовими точками, які представляють фактичне положення ключових точок у просторі пікселів зображення, ім’я яких містить позначку для ключової точки, а саме «rightEye», «leftEye», «noseTip», «mouthCenter», «rightEarTragion» і «leftEarTragion» відповідно, передається на вхід до іншої моделі яка відповідає за подальшу обробку та ідентифікацію, цього детектованого обличчя в системі.

3.2 Тренування розробленої моделі

Тренування моделі відбувалось за допомогою датасету з набором даних із 66-ти тисяч зображень. Для оцінки було використано географічно різноманітний набір даних, що складається з 2 тисяч зображень. Для моделі з враховувалися лише обличчя, які займають понад 20% площі зображення через передбачуваний варіант використання.

Саме тренування моделі відбувалось за допомогою алгоритму градієнтного спуску [32], який наведений на наступному рисунку 3.3.

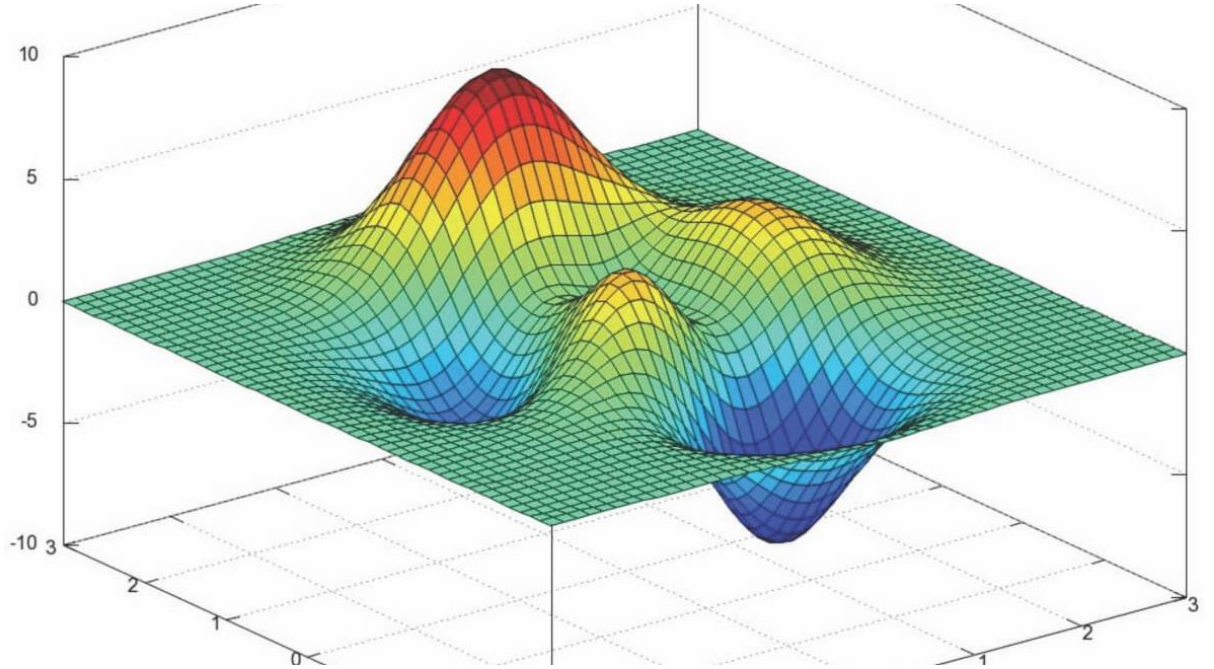


Рисунок 3.3 – Принцип алгоритму градієнтного спуску

Алгоритм градієнтного спуску ітеративно обчислює наступну точку, використовуючи градієнт у поточній позиції, масштабує її (за швидкістю навчання) і віднімає отримане значення з поточної позиції (робить крок). Він віднімає значення, тому що ми хочемо мінімізувати функцію (щоб максимізувати це було б додаванням).

Цей процес можна записати так:

$$p_{n+1} = p_n - n\nabla f(p_n)$$

Існує важливий параметр η, який масштабує градієнт і таким чином контролює розмір кроку. У машинному навчанні це називається швидкістю навчання та має сильний вплив на продуктивність.

Чим менша швидкість навчання, тим довше градієнтний спуск сходиться або може досягти максимальної ітерації до досягнення оптимальної точки. Якщо швидкість навчання надто висока, алгоритм може не сходитися до оптимальної точки (скакати) або навіть повністю розходитися.

Таким чином, загальні кроки методу градієнтного спуску, можна описати наступним планом, а саме:

– вибрати початкову точку (ініціалізація);

– обчислити градієнт у цій точці;
– зробити масштабований крок у протилежному напрямку до градієнта (мета: мінімізувати);
– повторювати пункти 2 і 3, доки не буде виконано один із критеріїв (досягнуто максимальної кількості ітерацій або коли розмір кроку буде менший за допуск, через масштабування або малий градієнт);

Слід зазначити, що на цьому етапі було звернуто увагу, на нормалізацію даних, перед тим як використовувати їх в моделі, оскільки якщо ми не нормалізуємо дані, то моделі прийдеться більше часу витрачати на градієнті спуски, взагалі модель може через це колапсувати, і якщо не робити нормалізацію, то прийдеться більше рухатись від однієї сторони до іншої, що може спричинити проблеми з продуктивністю моделі.

3.3 Тестування роботи розробленої системи детекції

Тестування роботи розробленої системи детекції обличчя проводилось в різних умовах, а саме:

– з різним освітленням в кімнаті (день / ніч);
– на різній відстані від камери;
– в звичайних умовах;
– в окулярах;
– в темноті;
– при закритих очах;
– при закритих частинах обличчя;
– при відсутності обличчя на камері;
– при наявності обличчя з фотографії;
– при наявності в камері декількох облич;

Нижче наведений перелік рисунків, як саме себе поводить система в різних умовах її використання.

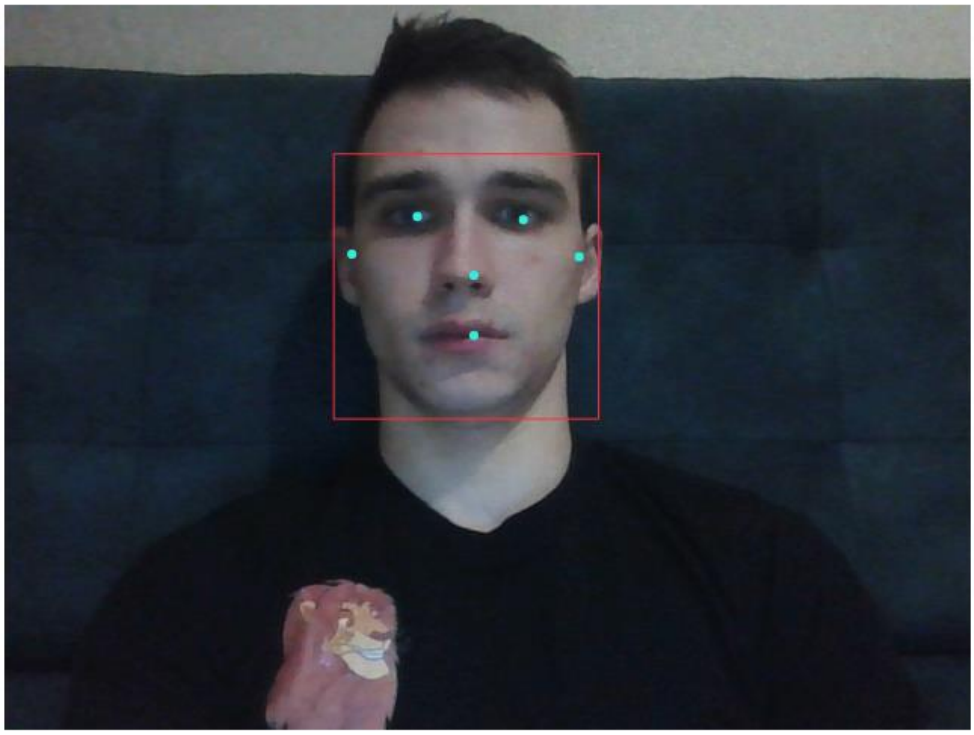


Рисунок 3.4 – Результат роботи системи детекції вночі

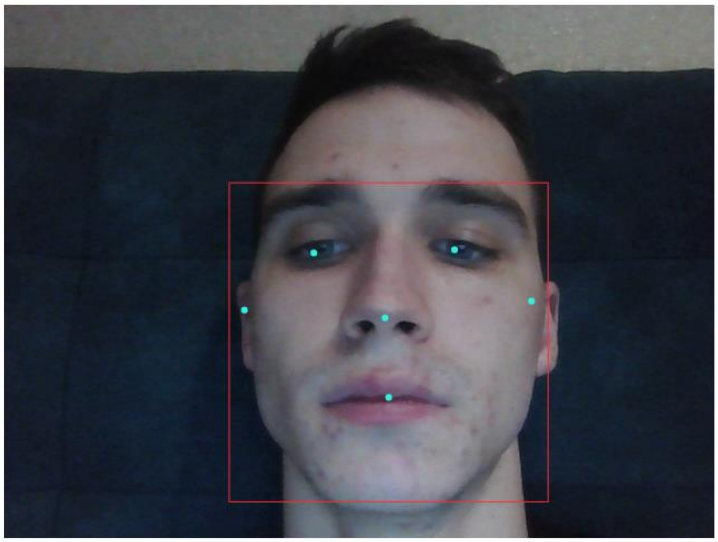


Рисунок 3.5 – Результат роботи системи детекції, коли користувач дуже близько біля камери

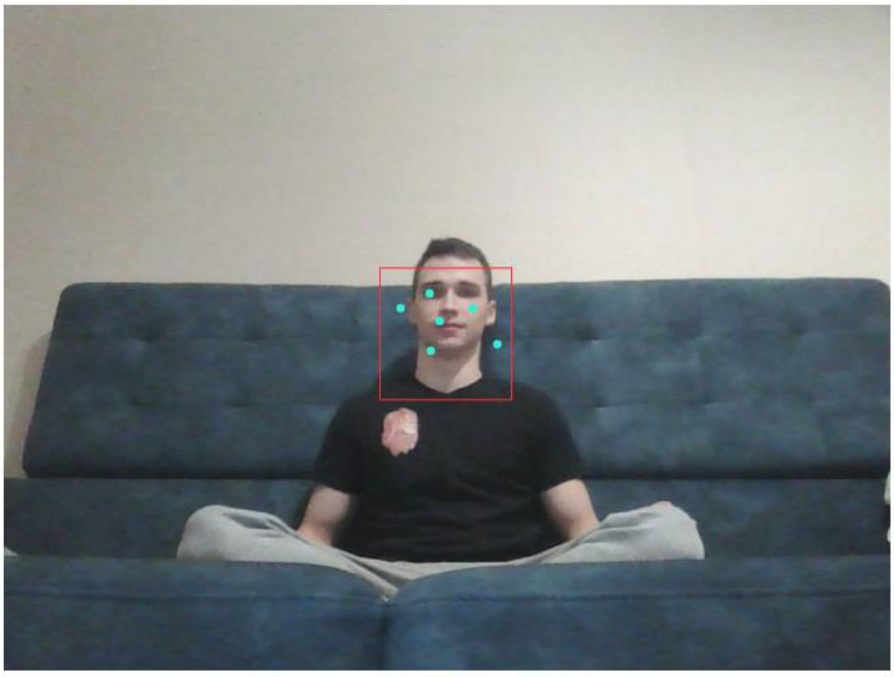


Рисунок 3.6 – Результат роботи системи детекції, коли користувач дуже далеко від камери

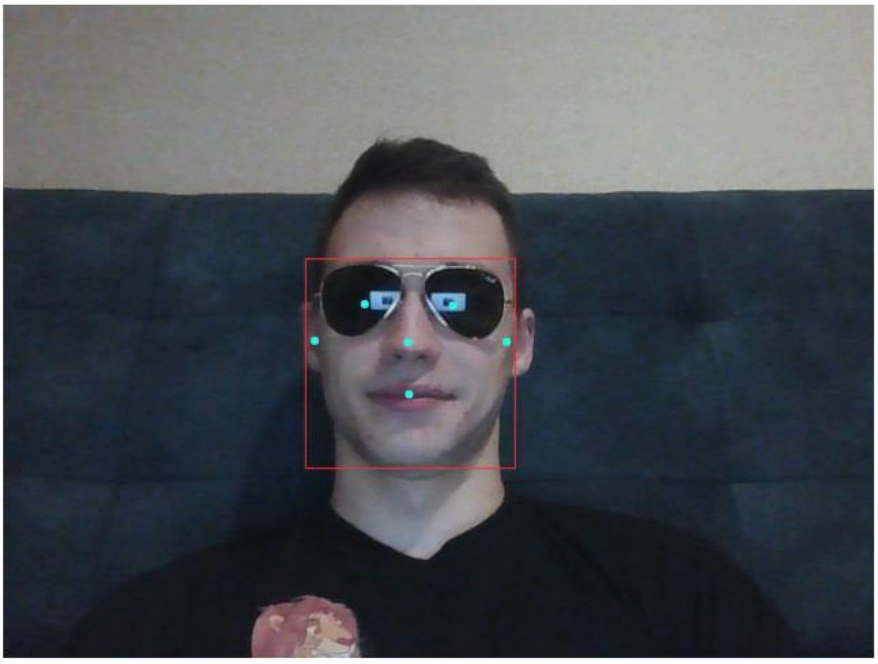


Рисунок 3.7 – Результат роботи системи детекції, коли користувач в окулярах

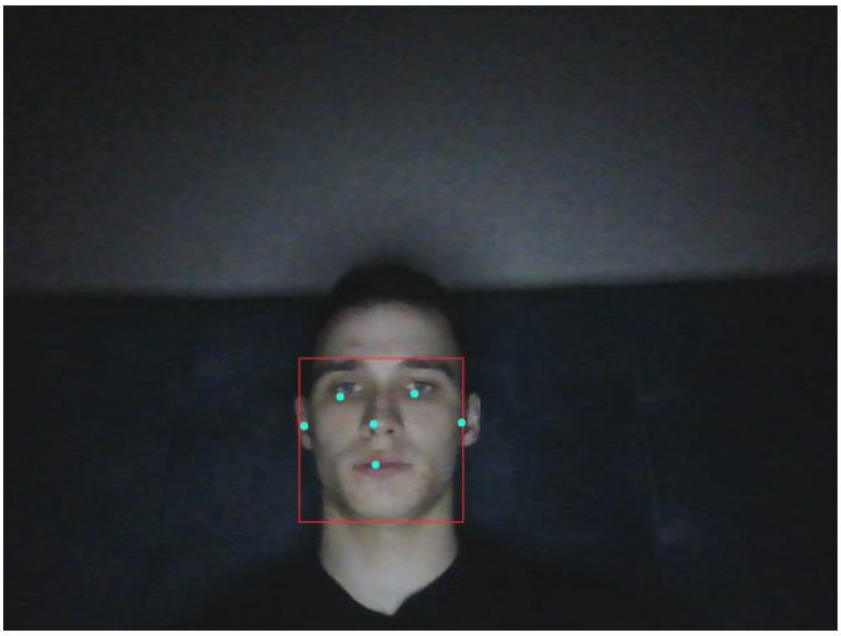


Рисунок 3.8 – Результат роботи системи детекції, коли користувач в темноті

Рисунок 3.9 – Результат роботи системи детекції, при закритому обличчі користувача

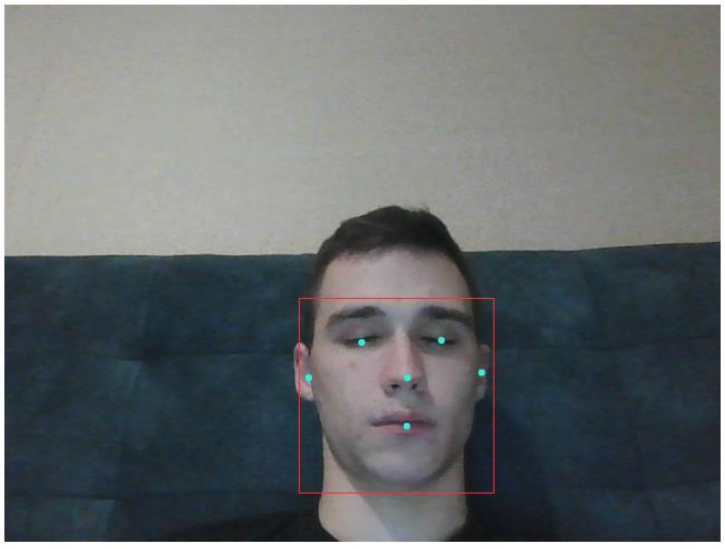


Рисунок 3.10 – Результат роботи системи детекції, із закритими очима

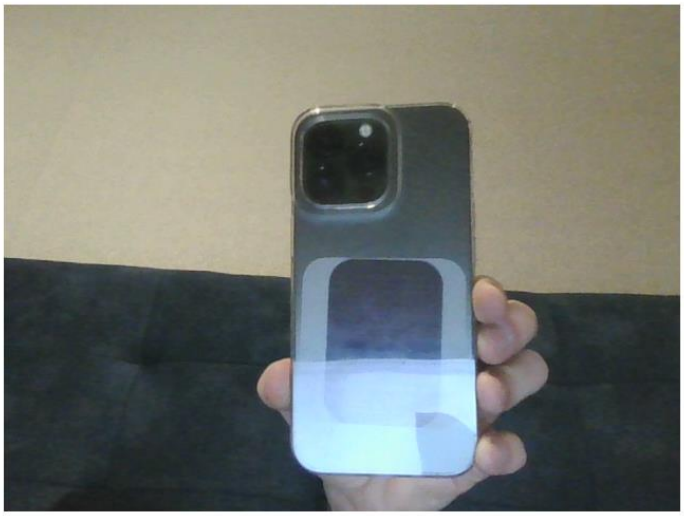


Рисунок 3.11 – Результат роботи системи детекції, із відсутнім обличчям

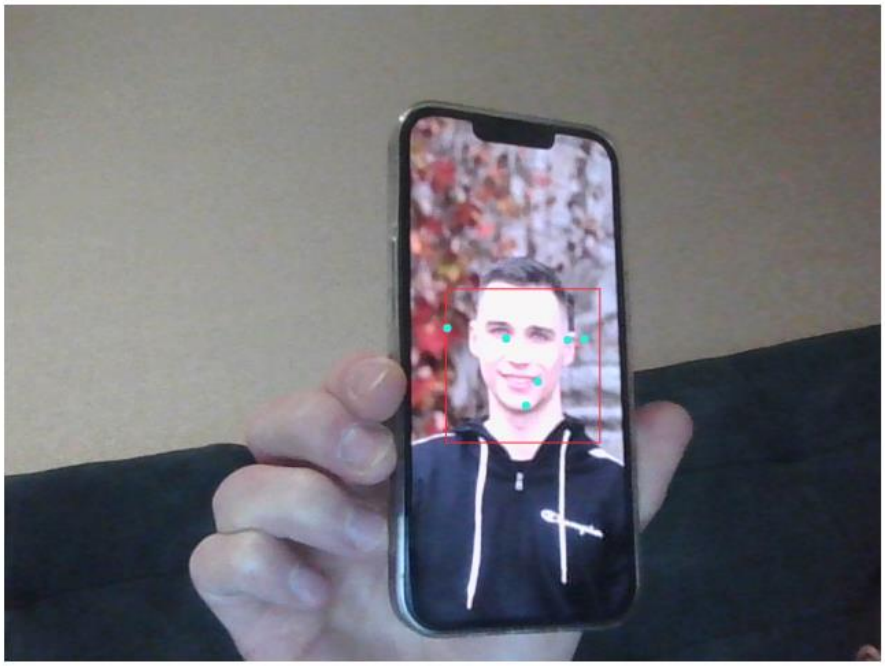


Рисунок 3.12 – Результат роботи системи детекції, із використанням обличчя з фотографії

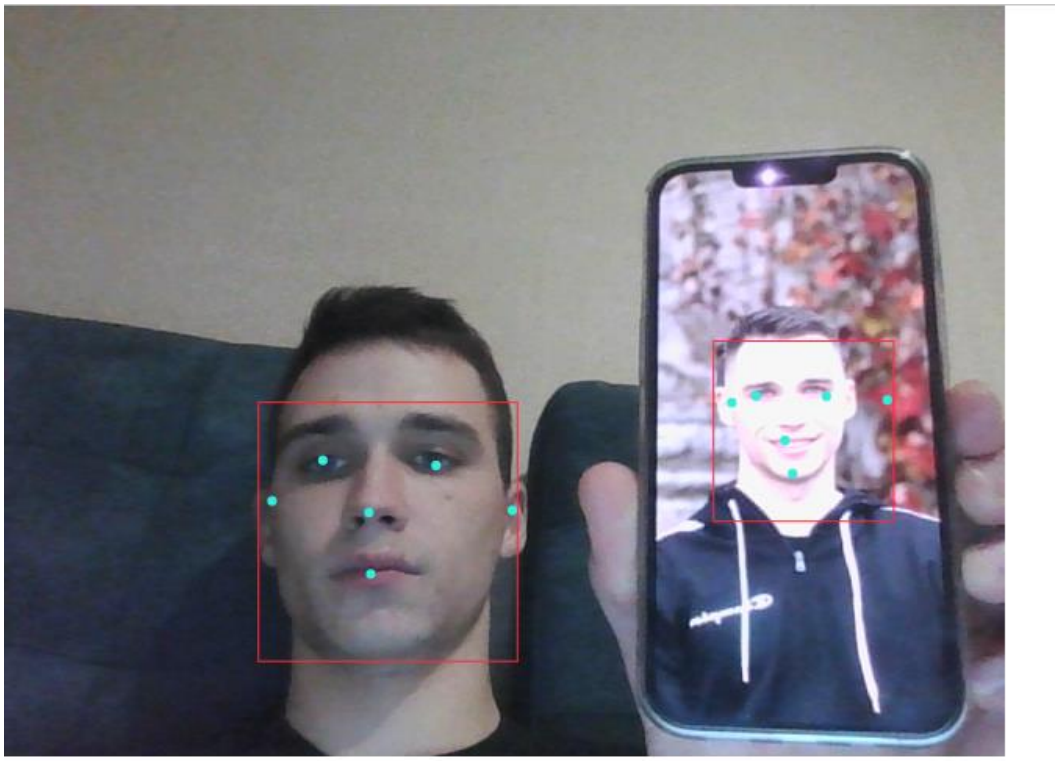


Рисунок 3.13 – Результат роботи системи детекції, при наявності декількох облич на зображенні

Отже, як бачимо, з рисунків наведених вище, розроблена система детекції показала себе досить непогано, навіть в різних не найкращих умовах для її використання, а саме в темноті, при наявності зайвих предметів на обличчі та при використанні обличчя з фотографії, проте незважаючи на ці умови, система відпрацювала успішно, що може свідчити про ефективність її роботи, проте у випадку з дуже далекою відстанню від камери, система не змогла розпізнати обличчя, як варіантом для вирішення такої проблеми може бути використання більш об’ємного датасету із наявністю в ньому зображень на далекій відстані.

3.4 Порівняння роботи методів та їх результатів

Також було виконано порівняння розробленого методу детекції обличчя користувача із існуючим методом детекції Dlib Frontal Face Detector [33]. Було розглянуто більш детально як працює цей метод та його суть.

Dlib — це набір інструментів C++, що містить алгоритми машинного навчання, які використовуються для вирішення реальних проблем.

Фронтальний детектор обличчя, наданий dlib, працює з використанням функцій, отриманих за допомогою гістограми орієнтованих градієнтів (HOG), які потім передаються через SVM (Support Vector Machine).

Загалом описаний вище метод детекції обличчя володіє наступними характеристиками:

– точність – 88%;
– час детекції обличчя користувача – 2-3с;
– можливість детекції декількох облич – наявна;
– підтримка мобільних девайсів – відсутня;

Далі для порівняння було виконано аналіз методу, який був розроблений під час виконання магістерської кваліфікаційної роботи. Для того, щоб визначити точність роботи методу, було проведено його тестування в різних умовах, та з різними користувачами.

Таблиця 2 – Точність роботи розробленого методу в різних умовах

Умова	Точність %	Користувачі
Користувач в окулярах	87, 93, 90	Володимир, Леонід, Андрій
Погане освітлення	67, 59, 61	Володимир, Леонід, Андрій
Користувач із закритими очима	90, 88, 84	Володимир, Леонід, Андрій
Частина обличчя в користувача закрита	66,52,55	Володимир, Леонід, Андрій
При наявності декількох облич	89, 90, 81	Володимир, Леонід, Андрій
При наявності обличчя з фотографії	87,89, 80	Володимир, Леонід, Андрій
Вночі	60, 53, 51	Володимир, Леонід, Андрій
При нормальній відстані від камери	94, 88, 92	Володимир, Леонід, Андрій
При далекій відстані від камери	70,76,78	Володимир, Леонід, Андрій

На основі наведеної вище таблиці, можна визначити що, ефективність роботи методу, є досить високою, а саме 92%, проте при гірших умовах, так як висока віддаленість від камери, або погане освітлення, ефективність розробленого методу погіршується, але система незважаючи на це, все ж таки продовжує працювати.

Загальний аналіз характеристик та статистика правильності роботи по приведеним системам детекції обличчя користувача наведена в наступній таблиці.

Таблиця 3 – Порівняння результатів розробленої системи з результатами іншої системи

Назва/Автор	Метод розроблений власноручно	Dlib Frontal Face Detector
Точність	92%	88%
Час детекції обличчя користувача	до 1.5с	2-3с
Можливість детекції декількох облич	+	-
Підтримка мобільних девайсів	+	-
Стабільна робота в поганих умовах	+	-

Проведений аналіз методу розробленого під час виконання магістерської кваліфікаційної роботи та методу детекції користувача, що був описаний вище, дозволяє зробити наступні висновки:

– метод, який розроблений під час виконання магістерської кваліфікаційної роботи дозволяє досягти більш високої швидкості реєстрації користувача в системі ніж метод Dlib Frontal Face Detector;

– розроблена власноруч метод, не викликає дуже високого навантаження на CPU, що дозволяє використовувати його в подальшому для роботи на мобільних девайсах;

– система, що розроблялась при виконанні магістерської кваліфікаційної роботи використовує сучасні бібліотеки для побудови моделі та роботи з нею,

що дозволило досягнути більш високої продуктивності роботи та більшої точності її роботи;

– система, що розроблялась при виконанні магістерської кваліфікаційної роботи, показала себе досить непогано в стресових умовах для її роботи, а саме при поганому освітленні та при високій віддаленості користувача від камери, що свідчить про її високу надійність.

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 1. Модуль детекції.» 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 1. Модуль детекції.» 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 **[Козловський, Лесько, Кавецький]**.

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 аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
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 ринку	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 використовуютьс я 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	4
2. Ринкові переваги (наявність аналогів)	2	2	2
3. Ринкові переваги (ціна продукту)	1	1	1
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	4	4
Сума балів	36	39	38
Середньоарифметична сума балів $СБ_c$	37,7		

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 **[Козловський, Лесько, Кавецький]**.

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 1. Модуль детекції.» становить 37,7 бала, що,

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

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 [34]:

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

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:

$$\beta_i = \frac{I_{нi}}{I_{ai}} \,, \qquad (4.2)$$

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

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

$$\beta_i = \frac{I_{ai}}{I_{ni}}; \qquad (4.3)$$

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	0,35
Швидкість ідентифікації об'єкта	с	0,8	0,3	2,67	0,2
Універсальність системи	бал	6,1	8,5	1,39	0,05
Точність ідентифікації об'єкта	%	78	85	1,09	0,25
Зручність інтерфейсу користувача	бал	5	8	1,6	0,15

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

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 1{,}09 \cdot 0{,}35 + 2{,}67 \cdot 0{,}2 + 1{,}39 \cdot 0{,}05 + 1{,}09 \cdot 0{,}25 + 1{,}6 \cdot 0{,}15 = 1{,}50.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,50 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 1. Модуль детекції.», 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 [35]:

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

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=24 дні.

$$З_о = 18200{,}00 \cdot 24 / 24 = 18200{,}00 \; грн.$$

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	758,33	24	18200,00
2. Ст. науковий співробітник проблем програмного забезпечення	18000,00	750,00	24	18000,00
3.Інженер-програміст	17500,00	729,17	24	17500,00
4. Аналітик систем обробки графічних даних	18000,00	750,00	10	7500,00

5. Консультант-аналітик обробки цифрових зображень	17500,00	29,17	5	3645,83
Всього				64845,83

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 1. Модуль детекції.» розраховуємо за формулою:

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

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:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \,, \tag{4.6}$$

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

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [35];

K_c – 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.

T_p – середнє число робочих днів в місяці, приблизно T_p = 24 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (24 \cdot 8) = 63{,}34$ *грн.*

$З_{р1} = 63{,}34 \cdot 12{,}00 = 760{,}03$ *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	12,00	2	1,10	63,34	760,03
2.Інсталяція програмного забезпечення	8,00	3	1,35	77,73	621,84
3.Встановлення цифрових обчислювальних систем	3,20	5	1,70	97,88	313,23
4. Відлагодження інтерполяційних модулів графічної системи	1,50	4	1,50	86,37	129,55
5. Підготовка цифрової експериментальної моделі ідентифікації	8,00	4	1,50	86,37	690,94
6. Формування бази даних підсистеми розпізнавання	12,00	2	1,10	63,34	760,03
7. Формування бази даних для підсистеми ідентифікації	12,00	2	1,10	63,34	760,03
8. Узгодження параметрів системи комп’ютерної графіки для формування реалістичних зображень	4,00	3	1,35	77,73	310,92
9. Тренування системи	4,00	3	1,35	77,73	310,92
Всього					4657,49

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 11%.

$З_{дод}$ = (64845,83 + 4657,49) · 11 / 100% = 7645,37 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 = (64845,83 + 4657,49 + 7645,37) · 22 / 100% = 16972,71 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 1. Модуль детекції.».

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

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

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.

$М_1$ = 3,0 · 207,00 · 1,1 - 0 · 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	-	-	683,10
Папір для заміток (А5)	130,00	4,0	-	-	572,00
Начиння канцелярське	200,00	3,0	-	-	660,00
Органайзер офісний	237,00	3,0	-	-	782,10
Картридж для принтера	1052,00	1,0	-	-	1157,20
Диск оптичний (CD-R)	20,00	3,0	-	-	66,00
Диск оптичний (CD-RW)	21,00	1,0	-	-	23,10
FLASH-пам'ять (16 ГБ)	110,00	1,0	-	-	121,00
FLASH-пам'ять (32 ГБ)	175,00	1,0	-	-	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 1. Модуль детекції.», 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, ($К_j = 1,1 \ldots 1,15$).

$К_в = 1 \cdot 8670,00 \cdot 1,1 = 9537,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.8 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Графічний адаптер: - тип відеокарти Дискретна - відеокарта nVidia Geforce 1650ti - об'єм відеопам'яті 4 ГБ	1	8670,00	9537,00
Всього			9537,00

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.

$B_{спец} = 38790,00 \cdot 1 \cdot 1,1 = 42669,00$ *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
Ноутбук Lenovo IdeaPad 15IMH05 Процесор: - Intel Core	1	38790,00	42669,00

i7-7820HQ (3,9 ГГц) - кількість ядер: 6 ядер			
Оперативна пам'ять: - оперативна пам'ять 32 ГБ - тип оперативної пам'яті DDR4	1	5760,00	6336,00
Всього			49005,00

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.

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.

$B_{прг} = 7908,00 \cdot 1 \cdot 1,1 = 8698,80$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.10 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Прикладне програмне забезпечення розробки	1	7908,00	8698,80
Середовище розробки: - WebStorm	1	720,00	792,00
Всього			9490,80

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.

$A_{обл} = (41560{,}00 \cdot 2) / (2 \cdot 12) = 3463{,}33$ *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
Програмно-аналітичний комплекс	41560,00	2	2	3463,33
Графічно-обчислювальний комплекс обробки даних	40720,00	2	2	3393,33
Програмні продукти обробки графічних даних	7945,00	2	2	662,08
Мультимедійна проекційна система	21790,00	4	2	907,92
Місце оператора спеціалізоване	8430,00	5	2	281,00

Офісна оргтехніка	7300,00	5	2	243,33
Дослідницька лабораторія	570000,00	20	2	4750,00
Прикладний пакет Microsoft Office 2016	7825,00	2	2	652,08
ОС Windows 10	8120,00	2	2	676,67
Всього				15029,75

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, $\eta_i < 1$.

$B_e = 0,32 \cdot 200,0 \cdot 6,20 \cdot 0,95 / 0,97 = 396,80$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.12 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Програмно-аналітичний комплекс	0,32	200,0	396,80
Графічно-обчислювальний комплекс обробки даних	0,15	200,0	186,00
Мультимедійна проекційна система	0,20	15,0	18,60
Місце оператора спеціалізоване	0,12	200,0	148,80

Офісна оргтехніка	0,62	3,2	12,30
Ноутбук Lenovo IdeaPad 15IMH05 Процесор: - Intel Core i7-7820HQ (3,9 ГГц) - кількість ядер: 6 ядер	0,04	200,0	49,60
Всього			812,10

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 1. Модуль детекції.» 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» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

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

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 25%.

$В_{св}$ = (64845,83 + 4657,49) · 25 / 100% = 17375,83 грн.

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» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

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

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$В_{сп}$ = (64845,83 + 4657,49) · 30 / 100% = 20851,00 грн.

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:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.17)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 75%.

$І_в$ = (64845,83 + 4657,49) · 75 / 100% = 52127,50 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:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.18)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 110%.

$В_{нзв}$ = (64845,83 + 4657,49) · 110 / 100% = 76453,66 грн.

Витрати на проведення науково-дослідної роботи на тему «Моделі та методи для детекції та ідентифікації обличчя користувачів комп'ютерних систем.

Частина 1. Модуль детекції.» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.19)$$

$B_{заг}$= *64845,83 +4657,49 +7645,37 +16972,71266 +4257,00 +9537,00 +49005,00 + 9490,80 + 15029,75 +812,10 +17375,83 +20851,00 +52127,50 +76453,66 = =349061,04 грн.*

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

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.20)$$

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

ЗВ = 349061,04 / 0,95 = 367432,68 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 1. Модуль детекції.» 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 855,53 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 [35]:

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.21)$$

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 $\rho = 35\%$;

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

Збільшення чистого прибутку 1-го року:

$\Delta П_1 = (855{,}53 \cdot 5300{,}00 + 16645{,}53 \cdot 550) \cdot 0{,}83 \cdot 0{,}35 \cdot (1\text{-}0{,}18/100\%) = 3260933{,}21$ грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2 = (855{,}53 \cdot 5300{,}00 + 16645{,}53 \cdot 1425) \cdot 0{,}83 \cdot 0{,}35 \cdot (1\text{-}0{,}18/100\%) = 6730422{,}41$ грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 = (855{,}53 \cdot 5300{,}00 + 16645{,}53 \cdot 2350) \cdot 0{,}83 \cdot 0{,}35 \cdot (1\text{-}0{,}18/100\%) = 10398168{,}13$ грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4 = (855{,}53 \cdot 5300{,}00 + 16645{,}53 \cdot 3100) \cdot 0{,}83 \cdot 0{,}35 \cdot (1\text{-}0{,}18/100\%) = 13372016{,}02$ грн.

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

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.22)$$

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, $\tau = 0{,}24$;

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

$ПП$ =3260933,21/(1+0,24)[1]+6730422,41/(1+0,24)[2]+10398168,13/(1+0,24)[3]+
+13372016,02/(1+0,24)[4]=2629784,85+4377225,81+5453706,73+5656009,72=
=18116727,11 грн.

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

$$PV = k_{інв} \cdot ЗВ, \tag{4.23}$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2,5;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 367432,68 грн.

$PV = k_{інв} \cdot ЗВ$ = 2,5 · 367432,68 = 918581,70 грн.

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

$$E_{абс} = ПП - PV \tag{4.24}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 18116727,11 грн;

PV – теперішня вартість початкових інвестицій, 918581,70 грн.

$E_{абс} = ПП - PV$ = 18116727,11 - 918581,70 = 17198145,42 грн.

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

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.25}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 17198145,42 грн;

PV – теперішня вартість початкових інвестицій, 918581,70 грн;

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

$$E_{в} = \sqrt[T_{ж}]{1 + \frac{E_{абс}}{PV}} - 1 = (1+17198145,42/918581,70)^{1/4} = 1,11.$$

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

$$\tau_{мін} = d + f, \tag{4.26}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d =0,12;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,32.

$\tau_{мін}$ = 0,12+0,32 = 0,44 < 1,11 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 1. Модуль детекції.» доцільно.

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

$$T_{ок} = \frac{1}{E_{в}}, \tag{4.27}$$

де $E_{в}$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 1,11 = 0,90 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 1. Модуль детекції.» становить 37,7 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 1,50 рази.

Також термін окупності становить 0,90 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 1. Модуль детекції.».

ВИСНОВКИ

У ході роботи над магістерською кваліфікаційною роботою було поставлено ряд проміжних завдань. Результати виконання кожного з них дозволили реалізувати систему, який цілком відповідає вимогам, поставленим у технічному завданні та реалізує детекцію обличчя користувача в системі за допомогою нейромереж. Проаналізувавши відомі системи для детекції обличчя користувачів, було знайдено їх певні недоліки чим обґрунтовано необхідність покращення швидкості роботи системи та точності правильної детекції обличчя користувача. Детальний аналіз літературних джерел показав, що використання сучасних нейромережевих структур зможе підвищити швидкодію системи в цілому. Тому було розглянуто актуальні нейромережеві структури та функції їх активації, і виконано їх аналіз. На основі цього аналізу було вирішено використовувати модель blazeface та функцію активації relu, адже використання цієї моделі дозволяє ефективно взаємодіяти з довгостроковими залежностями, і одночасно забезпечує достатню швидкодію при роботі з даними. Для розробленої системи детекції обличчя користувача було побудовано її узагальнену структуру роботи та виконано аналіз із структурним представленням її компонентів. У якому, розроблена система складається з таких блоків, як: блок попередньої обробки, блок детекції обличчя та блок подальшої обробки.

Також відповідно до розробленої узагальненої структури роботи було створено схему узагальненого алгоритму системи та виконано розробку алгоритмів роботи її компонентів. Реалізація програми була виконана за допомогою мови програмування JavaScript та бібліотеки TensorFlow, яка використовувалась для спрощення створення нейронних мереж та їх навчання, і середовища для розробки WebStorm. Окрім цього проведено тестування коректності роботи додатку, під час якого не було виявило ніяких недоліків реалізації, тому можна сказати, що тестування пройшло успішно. Система, яку було отримано в результаті виконання даної магістерської кваліфікаційної

роботи можна використовувати в інших системах для ідентифікації користувача і підтвердження його особи, адже алгоритм який реалізований у даній системі, достатньо швидкодійний та гарантує правильність та точність результату, при ідентифікації. Результати роботи системи були порівняні з результатами роботи іншої системи для детекції обличчя користувача, після порівняння було визначено, що система, яка розроблена у ході роботи над магістерською кваліфікаційною роботою, більш швидкодійна та має кращі результати, що ще раз підтверджує актуальність її використання.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гроувер Д, Сатер Р., Фіпс Д. Захист програмного забезпечення. 1992.
2. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації URL: https://ela.kpi.ua/bitstream/123456789/9839/1/26.pdf (дата звернення: 05.10.2022).
3. Nanavati S., Thieme M., Raj N. Biometrics: Identity Verification in a Networked World. 2002. URL: https://www.researchgate.net/publication /234758144_Biometrics_Identity_Verification_in_a_Networked_World (дата звернення: 05.10.2022).
4. Chandran G. C., Rajesh. R.S. Performance Analysis of Multimodal Biometric System Authentication. 2009. URL: http://paper.ijcsns.org/07_book/200903/20090340.pdf (дата звернення: 05.10.2022).
5. Galande S. G., Agrawal G.H., Pund D. D. Analysis of various Bio-metric Techniques. 2016. URL: https://www.ijareeie.com/upload/2016/ september/70_Dipali%20Pund.pdf (дата звернення: 05.10.2022).
6. Matthew A. T., Pentland A. P. Face Recognition Using Eigenfaces. URL: http://www.mit.edu/~9.54/fall14/Classes/class10/Turk%20Pentland%20Eigenfaces.pdf (дата звернення: 05.10.2022).
7. R. A. Fisher. The statistical utilization of multiple measurements, 1938.
8. P.J. Phillips. Support vector machines applied to face recognition, 1998.
9. B. Moghaddam, A. Pentland. Probabilistic visual learning for object representation, 1997.
10. M. Bartlett, Stewart, J. Movellan, R. Sejnowski, J. Terrence. Face recognition by independent component analysis, 2002.
11. E. Fazl Ersi, J. S. Zelek. Local Feature Matching for Face Recognition, 2006.
12. L. Wiskott, J. M. Fellous, C. von der Malsburg. Face recognition by elastic bunch graph matching, 1997.

13. A. Lanitis, C. J. Taylor, T. F. Cootes. Automatic face identification system using flexible appearance models, 1995.
14. T. F. Cootes, G. J. Edwards, C. J. Taylor. Active appearance models, 2001.
15. S. H. Lin, S. Y. Kung, L. J. Lin. Face recognition/detection by probabilistic decision-based neural network, 1997.
16. Face Detection For Beginners. URL: https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9 (дата звернення: 05.10.2022.)
17. What is the C4.5 algorithm and how does it work?. URL: https://towardsdatascience.com/what-is-the-c4-5-algorithm-and-how-does-it-work-2b971a9e7db0 (дата звернення: 05.10.2022).
18. ML | Find S Algorithm. URL: https://www.geeksforgeeks.org/ml-find-s-algorithm/ (дата звернення: 05.10.2022).
19. Face recognition by elastic bunch graph matching. URL: https://ieeexplore.ieee.org/document/598235%3Fsection (дата звернення: 05.10.2022).
20. A Review on OpenCV. URL: https://www.researchgate.net/publication/280977983_A_Review_on_OpenCV (дата звернення: 05.10.2022).
21. Real-Time Face Detection Using MATLAB URL: https://www.electronicsforu.com/electronics-projects/software-projects-ideas/real-time-face-detection-using-matlab (дата звернення: 05.10.2022).
22. Selective Search for Object Detection | R-CNN. URL: https://www.geeksforgeeks.org/selective-search-for-object-detection-r-cnn/ (дата звернення: 05.10.2022).
23. SSD: Single Shot MultiBox Detector URL: https://www.researchgate.net/publication/337401161_Fundamental_Concepts_of_Convolutional_Neural_Network (дата звернення: 05.10.2022).
24. YOLO: Real-Time Object Detection Detector URL: https://pjreddie.com/darknet/yolo/ (дата звернення: 15.11.2022).
25. RefineDet: Single-Shot Refinement Neural Network for Object Detection. URL: https://medium.com/nerd-for-tech/review-refinedet-single-shot-refinement-neural-

network-for-object-detection-object-detection-5fc483449562 (дата звернення: 15.11.2022).

26. RetinaNet URL: https://paperswithcode.com/method/retinanet (дата звернення: 15.11.2022).
27. Understanding CNN (Convolutional Neural Network) URL: https://towardsdatascience.com/understanding-cnn-convolutional-neural-network-69fd626ee7d4#:~:text=CNN%20is%20a%20type%20of,features%20automatically%20for%20better%20classification (дата звернення: 15.11.2022).
28. Bazarevsky V., Kartynnik Y., Vakunov V. BlazeFace: Sub-millisecond Neural Face Detection. 2019. URL: https://arxiv.org/abs/1907.05047 (дата звернення: 15.11.2022).
29. Howard A., Menglong Z., Chen B. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. URL: https://arxiv.org/abs/1704.04861 (дата звернення: 15.11.2022).
30. Ren S., Kaiming H., Girshick R. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. URL: https://arxiv.org/abs/1506.01497 (дата звернення: 15.11.2022).
31. Convolutional Neural Networks (CNNs / ConvNets). URL: https://cs231n.github.io/convolutional-networks/ (дата звернення: 15.11.2022).
32. Gradient Descent in Machine Learning. URL: https://www.javatpoint.com/gradient-descent-in-machine-learning (дата звернення: 15.11.2022).
33. Face Detection Models: Which to Use and Why? URL: https://towardsdatascience.com/face-detection-models-which-to-use-and-why-d263e82c302c (дата звернення: 15.11.2022).
34. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа – Вінниця : ВНТУ, 2016. – 113 с.
35. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 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 1. Модуль детекції.

Автор роботи: Говорун Володимир Валерійович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 96,97%. Схожість – 4,03%.

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)

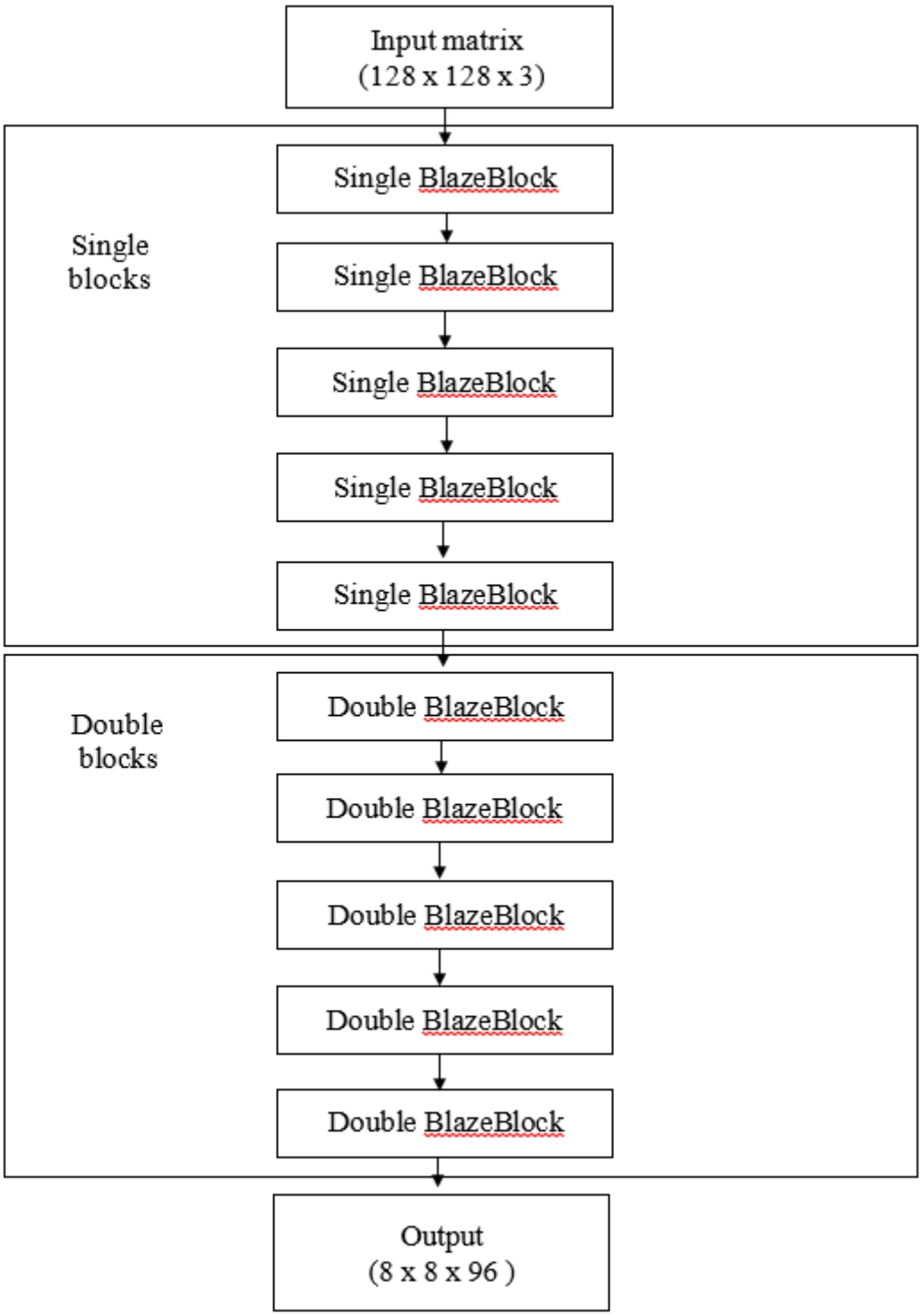
Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ _____
(підпис) (прізвище, ініціали)

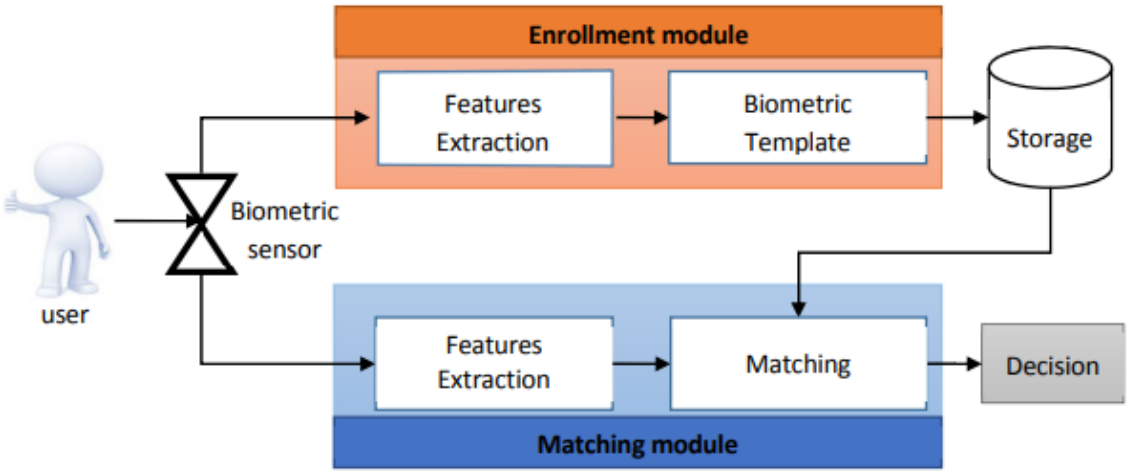
Керівник роботи _____ _____
(підпис) (прізвище, ініціали)

ІЛЮСТРАТИВНИЙ МАТЕРІАЛ

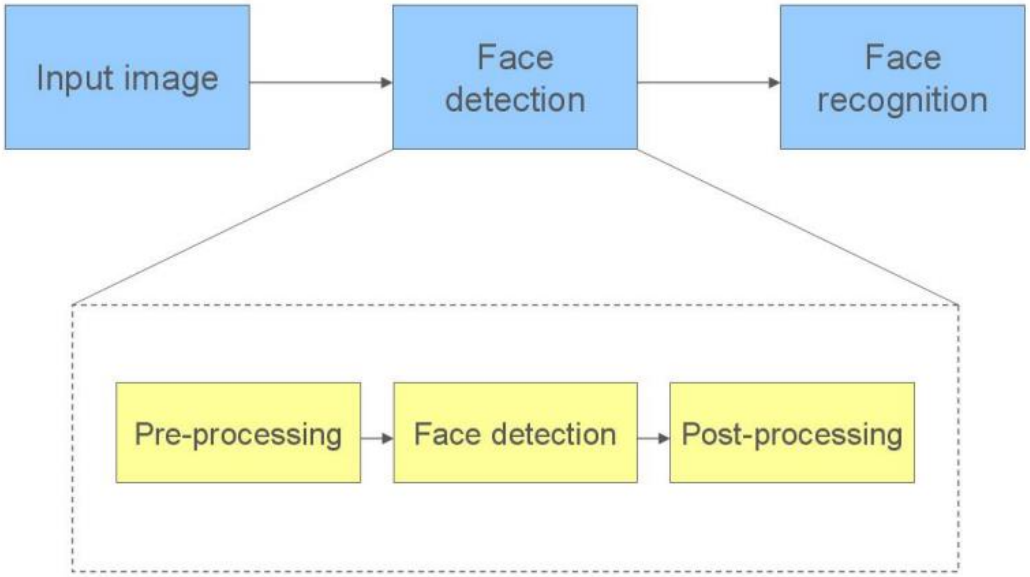
СТРУКТУРА МОДЕЛІ ДЕТЕКЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧА



ЗАГАЛЬНА АРХІТЕКТУРА СИСТЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА ОБЛИЧЧЯМ



ЗАГАЛЬНИЙ ВИГЛЯД МОДЕЛІ ІДЕНТИФІКАЦІЇ ОБЛИЧЧЯ КОРИСТУВАЧА



БЛОК СХЕМА РОБОТИ ПРОЦЕСУ ДЕТЕКЦІЇ

БЛОК СХЕМА РОБОТИ МОДУЛЮ ПОПЕРЕДНЬОЇ ОБРОБКИ ЗОБРАЖЕННЯ

СТРУКТУРА ПОДВІЙНОГО BLAZE БЛОКУ