МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК 004.932.72'1:004.056.53

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Засоби ідентифікації з використанням біометричних технологій у вебсередовищі

Виконавець:	Владислав ХРИСТЕВИЧ
Керівник: к.т.н., доцент	Іван ПАРХОМЕНКО
Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент	Тетяна ДМИТРУХА
Нормоконтролер: к.т.н., доцент	Іван ПАРХОМЕНКО

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютеризованих систем захисту інформації
_____ Михайло СТЕПАНОВ
«__» _____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
здобувача вищої освіти Христевича Владислава Богдановича

1. Тема: *Засоби ідентифікації з використанням біометричних технологій у вебсередовищі* затверджена наказом ректора від «15» вересня 2023 р. № 1814/ст.
2. Термін виконання: з 16.10.2023 р. по 31.12.2023 р.
3. Вихідні дані: нормативно-правова база в сфері захисту інформації, існуючі засоби біометричної ідентифікації; нейронні мережі штучного типу з поглибленим навчанням, алгоритми розпізнання об'єктів та бібліотеки вебтехнологій.
4. Зміст пояснювальної записки: аналіз нормативно-правової бази, функціональних аспектів та особливостей засобів біометричної ідентифікації згідно унікальних біометричних характеристик; аналіз існуючих нейронних згорткових штучних мереж та розробка вимог до ідентифікації по обличчю; розробка програмного модулю біометричної ідентифікації за допомогою вебтехнологій

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	*Виконано*
2.	Аналіз літературних джерел	18.10.2023-21.10.2023	*Виконано*
3.	Обґрунтування рішення	22.10.2023-24.10.2023	*Виконано*
4.	Збір інформації	25.10.2023-30.10.2023	*Виконано*
5.	Аналіз нормативно-правової бази	30.10.2023-31.10.2023	*Виконано*
6.	Дослідження та аналіз функціональних методів біометричної ідентифікації	01.11.2023-04.11.2023	*Виконано*
7.	Дослідження механізмів реалізації біометричної технологій	05.11.2023-08.11.2023	*Виконано*
8.	Вибір інструментальних засобів та технологій розробки	09.11.2023-10.11.2023	*Виконано*
9.	Розробка архітектури програмного модулю	10.11.2023-13.11.2023	*Виконано*
10.	Реалізація програмного модуля розпізнавання обличь	14.11.2023-30.11.2023	*Виконано*
11.	Оформлення і друк пояснювальної записки	05.12.2023	*Виконано*
12.	Оформлення презентації	10.12.2023	*Виконано*
13.	Отримання рецензій від рецензентів	22.12.2023	*Виконано*

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти Владислав ХРИСТЕВИЧ

(підпис, дата)

Керівник кваліфікаційної роботи Іван ПАРХОМЕНКО

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота на тему: «Засоби ідентифікації з використанням біометричних технологій у вебсередовищі» складається зі вступу, 4 розділів, загальних висновків, списку використаних джерел, додатку А, і має 74 сторінки основного тексту, 22 рисунки. Список використаних джерел містить 33 найменувань і займає 4 сторінки. Загальний обсяг роботи 83 сторінки.

Метою роботи є реалізація засобів біометричної ідентифікації на основі вебтехнологій.

В роботі вирішено наступні задачі:

- дослідження функціональних методів біометричної ідентифікації;
- аналіз проблем та вразливостей біометричної ідентифікації;
- дослідження механізмів реалізації біометричної технологій;
- реалізація програмного модуля розпізнавання обличь;
- тестування програмного модулю.

Отже, було проведено дослідження та порівняльний аналіз існуючих методів біометричної ідентифікації та технологій і засобів їх реалізації, а також розробка програмних засобів біометричної ідентифікації із використанням комбінованих програмних модулів, фреймворків та штучних нейронних мереж.

Ключові слова: біометрична ідентифікація, штучна згорткова нейронна мережа, алгоритм розпізнавання, програмна бібліотека, вебкамера, мова програмування, середовище функціонування, комп’ютерний зір, машинне навчання.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІТ – Інформаційні технології;

ІКТ – Інформаційно-комунікаційні технології;

ПЗ – Програмне забезпечення;

БД – База даних;

НСД – Несанкціонований доступ;

ІС – Інформаційна система;

АС – Автоматизована система;

ОС – Операційна система;

SSD – Детектор одиничного пострілу (Single Shot Detector);

CV – Комп’ютерний зір (Computer Vision);

API – Прикладний програмний інтерфейс (Application Programming Interface);

DCNN – Глибинна згорткова нейронна мережа (Deep Convolutional Neural Network);

CNN – Згорткова нейронна мережа (Convolutional Neural Network);

ANN – Штучна нейронна мережа (ШНМ, Artificial Neural Networks);

МН – Машинне навчання;

ПК – Персональний комп’ютер

ВСТУП

Актуальність. Технології сучасного світу невпинно розвиваються та надають нам можливість поліпшити та значно полегшити наше життя. Як показує практика та час набагато зручніше мати всю інформацію у цифровому вигляді, що значно пришвидшує роботу та полегшує контроль та розподіл цієї інформації поміж відповідних людей. Таким самим чином розвивається загроза для інформації. Засоби ідентифікації з використанням біометричних технологій у вебсередовищі вкрай актуальні в сучасному світі, існуючи на стику інформаційних технологій та безпеки. Досягнення в області біометричних технологій, таких як розпізнавання обличчя, відбитків пальців, структури руки, розпізнавання голосу та інші, роблять ці засоби ідентифікації надзвичайно потужними та надійними.

У світі, де онлайн-злочинність стає все більшою загрозою, біометричні технології можуть допомогти забезпечити вищий рівень безпеки веб-сервісів та додатків. Вони дозволяють підтверджувати особистість користувачів на основі їх унікальних біометричних даних, запобігаючи несанкціонованому доступу. Використання біометричних технологій дозволяє користувачам швидко та зручно автентифікуватися в системі, уникнувши необхідності запам’ятовувати паролі або використовувати інші засоби ідентифікації, що можуть бути вкрай надокучливими. Також вебсередовище є ключовим середовищем для банківських послуг і онлайн-торгівлі. Використання біометричних технологій допомагає підвищити рівень безпеки для клієнтів і знизити ризик фінансових злочинів. Законодавчі органи у багатьох країнах активно працюють над створенням рамок для використання біометричних технологій в цифровому просторі, зокрема, щодо захисту приватності користувачів. Це створює необхідність в розробці та впровадженні веб-систем, які відповідають вимогам законодавства.

Отже, засоби ідентифікації з використанням біометричних технологій у вебсередовищі є надзвичайно актуальною і важливою в сучасному світі інформаційних технологій та безпеки.

Метою роботи є реалізація засобів ідентифікації з використанням біометричних технологій у вебсередовищі. В роботі вирішено наступні задачі:

- дослідження методів та технологій біометричної ідентифікації;
- аналіз слабкостей та недоліків біометричної ідентифікації;
- дослідження механізмів реалізації біометричної технологій;
- реалізація програмного модуля біометричної ідентифікації;
- тестування програмного модулю.

Об’єкт дослідження: процес ідентифікації з використанням біометричних технологій у вебсередовищі.

Предмет дослідження: засоби ідентифікації суб’єкта з використанням біометричних технологій у вебсередовищі.

Новизна: було поєднано комбіновані нейронні та згортково нейронні мережі, комп’ютерний зоровий аналіз та машинне навчання для досягнення поставленої мети у ідентифікації суб’єкта у вебсередовищі.

Практична цінність полягає у тому, розроблений програмний модуль у вебсередовищі з комбінацією цих засобів підвищує стабільність та надійність систем надання доступу до інформації користувачам.

Галузь застосування. Дані засоби можуть застосовуватися у сфері захисту інформації інформаційно-комунікаційних систем та мереж, а саме для зниження ймовірності несанкціонованого доступу, підвищення точності авторизації та ідентифікації та забезпечення високого рівня захисту персональних даних.

Апробація. Христевич В. Б. "Комплексний метод біометричної ідентифікації в вебсередовищі", 2023 X International Conference "Information Technology and Implementation (Satellite)" (IT&I-2023), 78-79, Nov. 2023.

РОЗДІЛ 1. МЕТОДОЛОГІЯ ІДЕНТИФІКАЦІЇ ЗА БІОМЕТРІЄЮ

1.1 Біометрія та її регулятивні вимоги

Людина у своїй природі є унікальною і має свої особисті характеристики. Відбитки пальців, структура ДНК та інші фізіологічні і поведінкові особливості відрізняють кожну особу. Сучасні технології дозволяють використовувати ці характеристики не лише у медицині, але й у сфері кібербезпеки.

Біометрія – це процес ідентифікації або верифікації особи за допомогою автоматизованих методів, які базуються на її унікальних фізіологічних і поведінкових особливостях.

Сучасна біометрія відіграє достатньо велику роль у забезпеченні інформаційної безпеки. Багато підприємств використовують системи ідентифікації для контролю доступу користувачів, адміністраторів, працівникам та іншим особам що працюють у компанії чи користуються сервісами цієї компанії. . Управління доступом до цінних ресурсів та об’єктів є надзвичайно важливим аспектом у діяльності компаній, і забезпечення безпеки має високий пріоритет.

Багато компаній активно вдосконалюють інструменти для захисту інформації, такі як шифрування, створення одноразових (тимчасових) паролів, використання електронних підписів та видачу спеціальних цифрових сертифікатів. Проте на сьогоднішній день одним із найефективніших методів є комбінування цих заходів із передовими технологіями біометрії.

Біометрична ідентифікація включає два основних етапи:

1. Реєстрація: Під час цього етапу суб’єкт надає свої біометричні й унікальні дані та характеристики відповідно до обраного методу ідентифікації. За допомогою біометричних пристроїв проводяться вимірювання, і цифровий формат (шаблон або модель) біометричної характеристики вводиться в базу даних для конкретного користувача.

2. Розпізнавання: На другому етапі, біометрична характеристика, яка була зафіксована, проходить спеціальну обробку за допомогою спеціалізованої програми, щоб перетворитися в цифровий шаблон, який придатний для подальшого порівняння. Цей цифровий шаблон використовується для порівняння з іншими біометричними даними користувача під час спроби верифікації. Порівняння проводиться методом «зіставлення один до одного», і результат зазвичай виражається у вигляді числової ймовірності, що дана особа відповідає зареєстрованим біометричним характеристикам.

Ця система дозволяє використовувати унікальні характеристики кожної особи для надійної ідентифікації та забезпечення безпеки в доступі до ресурсів інформаційних систем.

Україна має чітку нормативну базу для обробки та експлуатацію біометричних даних з дотриманням принципів конфіденційності та захисту особистої інформації. Ця нормативна база включає такі закони:

- Закон України «Про положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства». Цей закон регулює використання біометричних даних для ідентифікації та верифікації осіб та встановлює правила збереження і захисту цих даних.
- Закон України «Про захист персональних даних». Цей закон встановлює загальні принципи обробки та захисту персональних даних, включаючи біометричні дані.
- Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». Цей закон визначає правила обробки даних, пов’язаних із громадянством та особистістю.
- Закон України «Про захист інформації в інформаційно-комунікаційних системах». Цей закон регулює заходи щодо захисту інформації, включаючи біометричні дані, в інформаційно-комунікаційних системах.

- Закон України «Про інформацію». Цей закон визначає правила доступу до інформації та обробки даних.
- Закон України «Про електронні документи та електронний документообіг». Цей закон встановлює правила створення, обробки та зберігання електронних документів, включаючи біометричні дані.

Ці закони забезпечують правовий фреймворк для обробки біометричних даних, зокрема забороняють обробку даних, які стосуються здоров'я, генетичних або біометричних даних без належної згоди та забезпечують захист основних прав і свобод людини і громадянина, включаючи право на конфіденційність та приватність.

Говорячи про вплив біометричної ідентифікації на суспільство та право в Україні то можна виявити деякі ключові аспекти цього впливу:

1. Забезпечення безпеки та боротьба зі злочинністю. Використання біометричної ідентифікації допомагає українським правоохоронним органам в боротьбі зі злочинами, включаючи шахрайства, підробку документів і тероризм. Біометричні дані можуть використовуватися для ідентифікації осіб на граничних пунктах та в органах правопорядку.
2. Зручність та безпека електронних послуг. Україна використовує біометричну ідентифікацію для надання громадянам доступу до електронних послуг, таких як електронний цифровий підпис, електронний візит до лікаря, онлайн-банкінг тощо. Це збільшує зручність та безпеку взаємодії з державними та комерційними організаціями.
3. Захист персональних даних і приватності. Використання біометричних даних підпадає під регулювання законодавства про захист персональних даних в Україні. Держава зобов'язана забезпечувати безпеку та конфіденційність цих даних, а також забороняє їхнє використання без належного дозволу осіб.
4. Імміграційний контроль та безпека кордонів. Біометрична ідентифікація використовується для контролю імміграції та безпеки на кордоні. Україна впровадила біометричні паспорти для своїх громадян і вимагає від

іноземців та осіб без громадянства надавати біометричні дані при в’їзді на територію країни.

5. Гендерні та етичні питання. Важливо враховувати, як біометрична ідентифікація впливає на гендерну рівність та може створювати стереотипи в обробці біометричних даних. Також виникають питання щодо етичних аспектів використання біометричних даних.
6. Міжнародні стандарти і співпраця. Україна враховує міжнародні стандарти у галузі біометричної ідентифікації, зокрема стандарти, розроблені Міжнародною організацією з нормалізації (ISO) і Міжнародною цивільною авіаційною організацією (ICAO), що сприяє міжнародній співпраці та обміну інформацією.

Також продовжуючи тему прав та свобод людини опишемо легітимність та етику використання біометрії.

Щодо легітимності:

- Законність та регулювання: Біометрична ідентифікація повинна проводитися відповідно до відповідних законів і нормативних актів, які регулюють обробку особистих даних та приватність. В Україні це може включати вимоги Закону «Про захист персональних даних».
- Згода і свобода вибору: Особи повинні мати можливість надавати свою згоду на використання своїх біометричних даних та повинні мати право відмовитися від цього виду ідентифікації без обмежень.
- Заборона дискримінації: Закон повинен запобігати будь-якій формі дискримінації на підставі біометричних характеристик, включаючи расу, стать, вік і інші особисті атрибути.

Щодо етики:

- Конфіденційність і безпека: Забезпечення конфіденційності і безпеки біометричних даних – це основний етичний аспект. Органи та організації, які збирають і обробляють біометричні дані, повинні здійснювати належний захист цих даних від несанкціонованого доступу та зловживань.

- Прозорість і відповідальність: Особи та організації, які використовують біометричну ідентифікацію, повинні бути прозорими щодо способів збору, зберігання та використання біометричних даних. Вони також повинні нести відповідальність за порушення прав та приватності осіб.
- Запобігання зловживанням: Біометричні системи не повинні використовуватися для незаконного або неетичного моніторингу чи переслідування осіб. Запобігання зловживанням та місцеві механізми захисту прав осіб є етичною вимогою.
- Доступність та рівні можливості: Важливо забезпечити доступність біометричних систем для всіх груп населення та уникнути створення бар'єрів для користувачів.
- Відсутність стереотипів і біасів: Розробники біометричних систем повинні активно працювати над уникненням стереотипів і біасів при аналізі біометричних даних, щоб не допустити несправедливих результатів.

1.2 Методи та технології біометричної ідентифікації особистості.

Біометрична ідентифікація включає в себе різноманітні методи підтвердження особистості, які можна поділити на дві основні категорії: статичні та динамічні.

Статичні методи базуються на фізіологічних особливостях особи, які є унікальними та не змінюються з часом. Ці методи включають:

1. Відбиток пальця. Це найбільш поширений метод, який ґрунтується на папілярних узорах пальця, які є унікальними для кожної людини. Відбиток, який був отриманий за допомогою сканера, аналізується та перетворюється на цифровий код, який в подальшому буде порівнюватися з зареєстрованим контрольним зразком.
2. Форма долоні. Цей метод ґрунтується на унікальній фізичній форми (геометрії) долоні, кисті або окремого пальця. З використанням спеціального пристрою, який складається з камери та діодів, створюється

тривимірне зображення долоні або пальця особи, яке потім аналізується для ідентифікації.

3. Інфрачервона камера. У даному методі використовується інфрачервона камера для сканування розташування вен на передній стороні долоні, кисті або пальця фізичної особи. Отримане зображення аналізується програмним забезпеченням і створюється відповідний цифровий ідентифікаційний шаблон.
4. Райдужна оболонка ока. Цей метод ґрунтується на унікальних рисах райдужної оболонки ока і не вимагає дорогого обладнання. Для сканування можна використовувати лише портативну камеру та спеціальне програмне забезпечення. Система виявляє обличчя на екрані, виділяє зображення ока та створює цифровий ідентифікаційний шаблон.
5. Сітківка ока. Ідея ідентифікації даного методу полягає у кровоносних судинах, які розташовані на очному дні. Дослідження очного дна застосовується в медицині. Для сканування потрібно піднести обличчя до медичного обладнання та виконати сканування камерою. При цьому людина повинна буде дивитися у різні боки задля повного сканування у різних положеннях ока.
6. Форма обличчя. Цей метод полягає в створенні двовимірного (2D) або тривимірного (3D) зображення обличчя, включаючи контури очей, губ, підборіддя, носа та інших рис. Використання тривимірної моделі обличчя є перспективним, оскільки воно надійніше для верифікації особи.
7. Термограма обличчя, рук чи пальця. Цей метод ґрунтується на унікальному розташуванні артерій на різних частинах тіла людини, яке створює тепловий фон. Для сканування використовуються камери інфрачервоного діапазону.
8. ДНК. Цей метод гарантує найвищу надійність, але вимагає багато часу і спеціального обладнання для аналізу ДНК.
9. Інші методи. Існує також досить багато інших цікавих методів, таких як сканування шкіряного шару, який розташований під нігтями,

ідентифікація за формою вуха, за запахом тіла і багато інших, які застосовуються за особливих обставин.

До динамічних методів біометричної ідентифікації відносяться такі способи:

1. Рукописний почерк. Робота даного методу базується на аналізі підпису фізичної особи. При написанні спеціального речення або кодового слова на планшеті або екрані з лазерним скануванням реєструються динамічні характеристики написання, такі як швидкість написання, стиль письма та сила з якою людина розписується на поверхні. Ідентифікація може проводитися як за порівнянням графічного образу підпису з базою даних, так і за динамічними даними написання.
2. Клавіатурний почерк. Цей метод включає в себе аналіз кодового слова (пароля), яке вводиться на клавіатурі. Параметри введення, такі як швидкість натискання на клавіші та інші динамічні характеристики, використовуються для створення ідентифікаційного шаблону. Даний метод не вимагає спеціального обладнання, адже використовує стандартну клавіатуру.
3. Голос. Цей метод використовує комбінацію частотних та статистичних параметрів голосу людини. Динамічні параметри голосу, такі як інтонація, тембр, і швидкість мовлення, аналізуються для ідентифікації особи. Для цього зазвичай використовуються спеціальні мікрофони та програмне забезпечення.
4. Електрокардіографія. Аналізується унікальний сигнал серцевої діяльності для ідентифікації особи. Може бути використаний для аутентифікації у реальному часі, важко підробити.
5. Електроенцефалограма. Аналізується активність мозку для ідентифікації особи. Дуже висока стійкість до шахрайства.
6. Інші методи. До інших методів, які використовують динамічні характеристики для ідентифікації особи, включають ідентифікацію за рухом губ під час вимови кодового слова або речення, за манерою ходи, за

динамікою обертання ключа у замковій свердловині дверей та інші подібні методи.

Біометрія в комп’ютерному зорі передбачає в основному поєднання обробки зображень і розпізнавання образів. Вона спеціалізується на розпізнаванні осіб на підставі фізіологічних характеристик, таких як обличчя, відбиток пальця, судинний малюнок або райдужна оболонка ока, а також на аналізі поведінкових рис, таких як хода чи мова.

Завдяки біометричним технологіям та комп’ютерному зору стає можливим забезпечення сучасних послуг розпізнавання, спостереження, захисту та допомоги, що є все більш важливими. Біометричні системи діють в різних сферах, які потребують збору візуальних, аудіо- та інших даних з датчиків для збору, розпізнавання, аналізу та керування очікуваними діями. Застосування біометричних технологій охоплює багато галузей, таких як охорона здоров’я, безпека, спостереження, виробництво, автомобільна промисловість та інші. Датчики, камери та мікрофони стають все безпечнішими, точнішими, надійнішими та вимагають інтеграції з адекватними функціями порівняння, перехресної перевірки та об’єднання.

Комп’ютерний зір використовує методи машинного навчання та глибокого навчання в підгалузях штучного інтелекту. Великий обсяг даних робить неможливим збереження огляду всіх тенденцій, змін та аспектів, що відбуваються в будь-який момент із найкращим розумінням. Тому для аналізу та еволюційного навчання, а також для швидкої та точної візуалізації чи спрацювання подій потрібна технологія штучного інтелекту.

Машинне навчання та комп’ютерний зір стали двома тісно пов’язаними галузями. Машинне навчання значно покращило комп’ютерний зір щодо розпізнавання та відстеження об’єктів. Воно надає ефективні методи для отримання, обробки зображень і фокусування на об’єктах, які використовуються в комп’ютерному зорі. Воно може навчатися без явного програмування.

З іншого боку, комп’ютерний зір розширив область машинного навчання. Він включає в себе цифрове зображення або відео, сенсорний пристрій, пристрій

для інтерпретації та стадію інтерпретації. Машинне навчання використовується в комп’ютерному зорі на стадії інтерпретації та інтерпретації. Глибоке навчання є ще кроком далі, коли сама мережа може адаптуватися до нових даних.

1.3 Аналіз вразливостей та недоліків біометричної ідентифікації.

Конфіденційна інформація завжди привертає увагу шахраїв, зловмисників та порушників, що створює значну загрозу в наш час. Зловмисники можуть використовувати різні методи, включаючи викрадення та продаж персональних даних та шантаж, щоб завдати шкоди. Дуже часто власники цієї інформації самі стають жертвами, внаслідок раптового забутого паролю, втрати блокнота з конфіденційною інформацією або навіть через використання біометричної ідентифікації за допомогою муляжу, створеного зловмисниками.

На сьогоднішній день, найбільший обсяг виготовлення муляжів припадає на біометричні пристрої, які використовують унікальні відбитки пальців. Це особливо актуально, оскільки метод використання відбитків пальців є надзвичайно поширеним. Наприклад, багато сучасних телефонів використовують функцію розблокування за відбитком пальця, де основним етапом є реєстрація свого власного відбитка пальця. Також, біометричні паспорти використовуються в державних підприємствах.

Загалом, процес створення дубліката відбитка пальців не є надто складним або витратним. Зловмисники та хакери здатні виготовити муляжі відбитків пальців, які можуть обхідно ввести в оману технології ідентифікації за відбитками. Наприклад, такий муляж можна створити з гелю. Основною метою є отримання відбитка пальця суб’єкта, який потім повинен доторкнутися до гладкого матеріалу, такого як чарка або фужер. Проте важливим фактором є чистота цього матеріалу для отримання більш точного відображення. Після цього залишається лише провести сканування поверхні та налаштувати контрастність, і на отриманому зображенні можна виготовити муляж відбитка пальця, використовуючи гель.

Проте найбільш небезпечним є викрадення біометричних даних після їх аналізу, сканування та внесення до бази даних. Біометричні дані можуть бути зафіксовані у формі зображення біометричних параметрів або у цифровому форматі, що створюється під час обробки цього зображення. В першому випадку існує значний ризик порушення конфіденційності особистих даних. Важливо відзначити, що методи шифрування також мають свої недоліки і можуть бути ненадійними. У такому випадку ніхто не може гарантувати відсутність викрадення даних, як механічних, так і програмних.

Ще однією слабкістю біометричної ідентифікації є процес ідентифікації за обличчям. У 2011 році компанія «Google» визнала, що технологія “Face Unlock”, яка була головним нововведенням у операційній системі (ОС) Android версії чотири, не функціонувала відповідно до очікувань. Проблема полягала в тому, що технологія не відрізняла фотографію обличчя користувача від живої особи. Іншими словами, систему можна було обдурити просто показуючи фотографію перед камерою телефону. Пізніше цю проблему вирішили завдяки новим оновленням “Face Unlock”.

Також важливо відзначити, що після надання суб’єктом своїх біометричних даних, ці дані можуть бути використані для різних цілей, з якими власник не надавав прав та не погоджувався. Наприклад, всі біометричні ознаки містять інформацію про стан здоров’я особи, включаючи фізіологічні та патологічні стані, а також неврологічні та судинні проблеми.

Крім того, особа, яка надала свою ДНК для ідентифікації, може бути під загрозою, оскільки зловмисники можуть використовувати її ДНК для підставного використання на місцях злочинів.

Можливість використання біометричних технологій значно обмежена в країнах третього світу, оскільки деякі пристрої та обладнання вимагають великих витрат та постійного технічного нагляду.

Ще однією проблемою є неможливість зміни біометричних характеристик у разі втрати або викрадення. Наприклад, коли пароль втрачається або псується, користувач може змінити його на новий, більш надійний. Проте в біометрії

змінити біометричні характеристики практично неможливо, що ставить під сумнів їх використання в аутентифікації та ідентифікації особистості.

Також варто зазначити проблеми біасу та дискримінації.

Біас вказує на систематичні відхилення або неточності у визначенні осіб за їхніми біометричними характеристиками. Це може стати результатом неправильного підбору даних для тренування алгоритмів розпізнавання або нерепрезентативного вибірку даних, які містять біометричні шаблони.

Дискримінація в біометричній ідентифікації може відбуватися, коли система неправильно визначає осіб на підставі їхньої раси, статі, віку, етнічності або інших особистих характеристик. Це може призводити до несправедливого обмеження доступу до послуг або надання пільг одній групі осіб перед іншою.

1.4 Висновки до першого розділу

Біометричні технології відкривають широкий спектр можливостей для захисту особистих даних та ідентифікації осіб. Ці методи можна розділити на дві основні категорії: статичні та динамічні.

Усі процедури збору біометричних даних в Україні повинні відповідати вимогам законодавства, таким як “Про положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства”, “Про захист персональних даних”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні документи та електронний документообіг”. Зібрані персональні біометричні дані, отримані за допомогою спеціальних пристроїв, не повинні розповсюджуватися без належного дозволу власника цих даних.

Як і в будь-якому виді ідентифікації, біометрична ідентифікація має свої проблеми та вразливості. Деякі з цих проблем загрожують цілісності та конфіденційності особистих даних та інформації, в той час як інші можуть

створювати загрозу для особистого життя особи, її стану здоров’я, різних видів захворювань і т. д.

РОЗДІЛ 2. РОЗГЛЯД МЕХАНІЗМІВ ВПРОВАДЖЕННЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

2.1 Взаємодія комп’ютерного зору та машинного навчання.

Комп’ютерний зір має на меті надати комп’ютерним системам можливості зорового сприйняття, схожі на людські. Це міждисциплінарна сфера, яка дозволяє комп’ютерним системам обробляти, аналізувати та точно інтерпретувати наш візуальний світ.

Наприклад, комп’ютерний зір дає змогу комп’ютерам ідентифікувати значущу інформацію із зображень і відео файлів так само, як це роблять люди. Мета полягає в тому, щоб надати цю «природну» візуальну характеристику комп’ютерам, щоб вони могли розуміти та аналізувати складні цифрові системи – так само, як це можуть люди – і, можливо, навіть краще. Сучасне комп’ютерне зір використовує машинне навчання, яке є компонентом штучного інтелекту, який зосереджується на «навчанні» машин навчатися самостійно з часом. Однак, на відміну від системи, яка завжди діятиме за попередньо визначеним набором правил або інструкцій, система машинного навчання аналізуватиме минулий досвід і рішення, щоб прийняти рішення про відповідну відповідь. Крім того, всього цього можна досягти з мінімальним втручанням людини або взагалі без нього.

Машинне навчання — це проста підмножина або частина штучного інтелекту. Без допомоги людини машини, які впроваджують машинне навчання, можуть автоматично аналізувати та розуміти цифрові дані. Машинне навчання зазвичай використовує як статистичні принципи, так і алгоритми для створення моделей, здатних виводити рішення на основі вхідних даних. Тому машинне навчання застосовується в кількох сферах, починаючи від суперкомп’ютерів і закінчуючи розробкою складного програмного забезпечення.

Контрольоване навчання надає комп’ютерам потужний набір інструментів для класифікації та інтерпретації цифрових даних. Щоб увімкнути

контрольоване навчання, цифрові дані потрібно позначити вручну. Потім цей позначений набір даних використовується як матеріал для навчання класифікації інших подібних немічених даних за допомогою алгоритмів машинного навчання.

Контрольоване навчання є важливою формою машинного навчання. Його називають контрольованим, оскільки процес навчання здійснюється з використанням попередньо отриманих міток спостережень, на відміну від навчання без контролю, де немає доступних даних, позначених вручну.

Що стосується набору навчальних даних, вхідні змінні є ключовими характеристиками, які впливають на точність прогнозованої мітки. Він міститиме як якісні, так і кількісні змінні, а вихідною змінною буде мітка (номер або клас).

Відповідно до різних типів вихідних змінних контрольовані навчальні завдання поділяються на дві різні категорії:

1. Класифікаційне завдання. Завдання класифікації: вихідна змінна завдання класифікації є категоріальною змінною. «Кішка» або «Собака» є прикладами можливих категорій завдання класифікації зображень.
2. Регресійна задача. Задача регресії: вихідна змінна неперервна. Прогнозований рух курсу акцій на фондовому ринку зазначається як завдання регресії.

Що саме таке комп’ютерний зір у машинному навчанні? Машинне навчання розширило здатність комп’ютерного зору правильно аналізувати візуальні дані шляхом швидкого визначення цифрових шаблонів. Машинне навчання зробило обробку зображень комп’ютерного зору позитивно ефективною завдяки характеристикам миттєвого розпізнавання та ефективній обробці цифрових зображень.

Комп’ютерний зір отримав значну користь від методів машинного навчання, які включають масштаб цифрових операцій машинного навчання. Ключові досягнення в процесах комп’ютерного зору дозволили алгоритмам машинного навчання працювати на більш широкому діапазоні цифрових наборів даних.

Машинне навчання та процедури комп'ютерного зору на основі штучного інтелекту були розроблені для правильної ідентифікації та діагностики пухлин та інших новоутворень, що з'являються в тілі людини. Незважаючи на те, що нещодавні результати застосування були обнадійливими, у цій галузі медицини завжди є місце для подальшого вдосконалення.

Основні відмінності між комп'ютерним баченням і машинним навчанням:

1. Технологічні відмінності:

- Комп'ютерне бачення – це технологія, яка намагається навчити комп'ютери впізнавати візуальні дані на зразок людини. З іншого боку, машинне навчання – це процес, який дозволяє комп'ютерам вчитися обробляти та реагувати на дані на основі попередніх дій. У кількох словах, машинне навчання є загальнішим і не обов'язково включає візуальні дані.

2. Різниця у фокусі:

- Як у випадку комп'ютерного бачення, так і в машинному навчанні мета полягає в тому, щоб комп'ютерні системи навчилися обробляти та реагувати на дані в конкретних ситуаціях. Проте комп'ютерне бачення набагато більше зосереджене на зображеннях та візуальних даних, тоді як машинне навчання фокусується на інших типах даних і спрямоване на вирішення завдань класифікації зображень, виявлення об'єктів, сегментації об'єктів, відстеження об'єктів на відео тощо. У обох випадках результат однаковий, проте тип вхідних даних визначає, який процес навчання працюватиме краще. Головною метою є можливість комп'ютерній системі вчитися на основі попередніх даних.

3. Де використовується комп'ютерне бачення?

- Комп'ютерне бачення використовується в різних сферах, включаючи медичну діагностику, сільське господарство та допоміжні системи для безпілотних автомобілів. В порівнянні з цим, машинне навчання також використовується, коли аналізуються дані на основі тексту або мовлення. Приклади таких застосувань включають в себе розпізнавання мови, аналіз

фінансових даних, аналіз даних про трафік, аналіз електронної пошти та застосунки у фінансових технологіях.

Застосування комп'ютерного зору з використанням машинного навчання:

1. Можливість розпізнавання в системі комп'ютерного зору. Це специфічне застосування машинного навчання в рамках комп'ютерного зору змінило технологічний ландшафт світу. Дивовижно бачити, як просте застосування машинного навчання в системах комп'ютерного зору може мати важливі наслідки.
2. Завдяки перекриттю компетенцій машинного навчання та комп'ютерного зору здійснюється обробка зображень на основі штучного інтелекту, за допомогою якої зображення даних маніпулюються або змінюються для покращення якості оригінального зображення або вилучення нової та актуальної інформації з оригінального зображення.
3. Це важливе застосування машинного навчання в рамках комп'ютерного зору використовується майже в кожній цифровій візуальній галузі:
    - Бізнес-аналітика та дослідження ринку,
    - Відображення 3D-даних,
    - Сільське господарство: і зокрема моніторинг посівів і продукції в режимі онлайн і в реальному часі для виявлення та запобігання хворобам,
    - Безпека: візуальне цифрове розпізнавання обличчя для систем безпеки та спеціально для аеропортів.
    - Розваги.

Ці приклади показують, наскільки критично важливим є збіг програм комп'ютерного зору та машинного навчання в реальному світі.

Комп'ютерне бачення на базі машинного навчання (або штучного інтелекту загалом) уже забезпечило величезні переваги та знайшло широке застосування в реальному світі.

Зараз процес виробництва автомобілів переважно роботизований. Ключові виробники автомобілів, такі як Mercedes, Tesla та BMW, значною мірою

перейшли на автоматизовані виробничі та складальні лінії. Лідери автомобільного бізнесу зрозуміли, що ефективність і результати скорочення витрат, які вони отримають від впровадження такого вдосконаленого комп'ютерного бачення, непорівнянні з іншими процесами та виробничими методами.

Дійсно, майже кожен процес автоматизації на таких складальних лініях функціонує в основному завдяки методологіям комп'ютерного зору на основі машинного навчання. Однак без ефективної сенсорної цифрової обробки зображень і нездатності систем машинного навчання інтерпретувати їх середовище та оточення інвестиції не відбудуться.

У наш час комп'ютерний зір значною мірою покладається на штучний інтелект, оскільки штучний інтелект постійно розширює сферу діяльності комп'ютерного зору та забезпечує додаткову ефективність обробки цифрових зображень комп'ютерного зору.

Іншим прикладом того, як підприємства використовують штучний інтелект, є використання ними автоматизації процесів на складах. Ключові організації електронної комерції, такі як Alibaba та Amazon, запровадили методи автоматизації на основі штучного інтелекту на своїх складах. Ці важливі системи виконують більшість своїх «комплектування та пакування» вибраних клієнтом продуктів.

Технічна «спорідненість» між комп'ютерним зором і штучним інтелектом дозволила корпораціям, які фінансували впровадження, варті уваги варіанти довгострокової економії. Наприклад, за допомогою своєчасних (або JIT) операцій із запасами підвищується ефективність і відчутні конкурентні переваги.

Підприємства починають усвідомлювати — і визнавати — потенціал комп'ютерного зору на базі штучного інтелекту для економії грошей і підвищення продуктивності.

Комп'ютерне бачення та машинне навчання є важливими аспектами ландшафту штучного інтелекту. Вони вже вдосконалили найсучасніші рівні

точності та продуктивності в кількох завданнях, таких як класифікація зображень, виявлення об’єктів і сегментація.

Крім того, поєднання комп’ютерного зору та машинного навчання оптимізує та спрощує створення ефективних технічних підходів, програм і систем для всіх основних галузей промисловості та бізнес-секторів.

Машинне навчання та комп’ютерне зір — це дві передові технічні галузі, які еволюціонували, щоб стати тісно пов’язаними. Машинне навчання покращило комп’ютерне бачення щодо відстеження та розпізнавання. Крім того, він пропонує ефективні методи збору даних, обробки цифрових зображень і фокусування об’єктів даних – методи, які всі використовуються в комп’ютерному зорі. Для порівняння, машинне навчання є ширшою технічною сферою, і її загальніші алгоритми можна використовувати в інших областях і сферах.

Взаємодія комп’ютерного зору і машинного навчання є ключовою для розпізнавання обличь в сучасних системах. Комп’ютерне зорове розпізнавання обличь є важливим завданням в області комп’ютерного бачення, і воно використовує різні методи та технології, включаючи машинне навчання, для досягнення високої точності та ефективності. Ось як ці дві галузі взаємодіють при розпізнаванні обличь:

1. Збір візуальних даних: Перший крок у розпізнаванні обличь полягає у зборі великих об’ємів візуальних даних. Це можуть бути фотографії, відеозаписи або навіть живий відео-потік. Збір візуальних даних важливий для створення навчальних наборів даних, які будуть використовуватися для навчання моделей.
2. Обробка візуальних даних: Вхідні візуальні дані піддаються обробці, щоб зменшити шум та підвищити якість зображень. Це може включати в себе розмиття, вирівнювання, видалення фону та інші операції, які полегшують аналіз обличь.
3. Виявлення обличь: Тут комп’ютерний зір використовується для виявлення обличь на візуальних даних. Моделі, навчені на великих навчальних

наборах, визначають положення та орієнтацію обличь на зображеннях або відео.

4. Визначення ключових точок: Після виявлення обличь, система використовує комп'ютерний зір для визначення ключових точок на обличчі, таких як очі, ніс, рот тощо. Це важливо для аналізу емоцій та ідентифікації особливостей.
5. Машинне навчання для розпізнавання: Найбільш критичним етапом є навчання моделей машинного навчання для розпізнавання обличь. Моделі використовуються для ідентифікації обличь та класифікації їх на основі попередньої навчальної інформації. Вони можуть використовувати різні архітектури глибокого навчання, такі як згорткові нейронні мережі (CNN) для розпізнавання обличь та оцінки ідентичності.
6. Застосування: Результати розпізнавання можуть бути використані для різних цілей, таких як розблокування смартфонів, розпізнавання обличь для безпеки, віртуальних середовищ, медичної діагностики, відеоспостереження, додатків для соціальних мереж та багато інших сфер.

Загалом, взаємодія комп'ютерного зору та машинного навчання дозволяє системам навчатися розпізнавати та аналізувати обличчя, визначати особливості та використовувати цю інформацію для різних завдань і застосувань. Це робиться за допомогою великої кількості даних та складних моделей, що поєднують у собі технології комп'ютерного зору та машинного навчання.

2.2 Методи розпізнавання обличчя.

В останні кілька років розпізнавання обличь приділяло значну увагу та оцінювалося як одне з найперспективніших застосувань у галузі аналізу зображень. Виявлення обличчя може займати значну частину операцій розпізнавання обличчя. Відповідно до його сили зосередити обчислювальні ресурси на ділянці зображення, що містить обличчя. Метод визначення обличчя на фотографіях є складним через різноманітність людських обличь, як-от поза,

вираз обличчя, положення та орієнтація, колір шкіри, наявність окулярів або волосся на обличчі, відмінності в підсиленні камери, умови освітлення та роздільна здатність зображення.

Виявлення об’єктів — це одна з комп’ютерних технологій, яка пов’язана з обробкою зображень і комп’ютерним зором і взаємодіє з виявленням екземплярів об’єктів, таких як людські обличчя, будівлі, дерева, машини тощо. Основна мета алгоритмів виявлення обличь — визначити чи є обличчя на зображенні чи ні.

Останнім часом було запропоновано багато досліджень у галузі розпізнавання обличь і виявлення обличь, щоб зробити їх більш досконалими та точними, але це стало революцією в цій галузі, коли Viola-Jones представила свій детектор обличчя, який здатний розпізнавати обличчя в режимі реального часу з високою точністю.

Розпізнавання обличчя є першим і важливим кроком для розпізнавання обличчя, і воно використовується для виявлення обличь на зображеннях. Це частина виявлення об’єктів і може використовуватися в багатьох сферах, таких як безпека, біометрія, правоохоронні органи, розваги, особиста безпека тощо.

Він використовується для виявлення обличь у режимі реального часу для спостереження та відстеження осіб або об’єктів. Він широко використовується у фотоапаратах для ідентифікації кількох зображень у кадрі камер Ex-Mobile та DSLR. Facebook також використовує алгоритм розпізнавання обличь, щоб розпізнавати обличчя на зображеннях.

Нижче наведено чотири популярні методи визначення обличчя:

На основі знань. Для того, щоб техніка, заснована на знаннях, могла розпізнавати обличчя, необхідно дотримуватися певних правил, і це залежить від людського розуміння. Наприклад, обличчя повинно мати ніс, очі та рот, які знаходяться на певній відстані та в певному положенні один від одного.

Коли справа доходить до цих стратегій, найбільш істотним недоліком є складність у розробці відповідного набору критеріїв. Якби критерії були або надто розпливчастими, або надто конкретними, могла бути велика кількість

помилкових спрацьовувань. Тільки цей метод є недостатнім і не здатний ідентифікувати кілька обличь на великій кількості фотографій.

На основі функцій. Техніка на основі ознак використовується для пошуку обличь шляхом вилучення структурних характеристик із обличь, які ідентифікуються. Спочатку він тренується як класифікатор, а потім використовується для розрізнення лицьових і нелицевих частин тіла.

Зрештою, мета полягає в тому, щоб подолати обмеження нашого інстинктивного усвідомлення облич. За словами авторів, ця стратегія, яка розділена на численні розділи та містить фотографії з кількома обличчями, має показник успіху до 95 відсотків.

Зіставлення шаблонів. Можна виявляти або розпізнавати обличчя за допомогою підходу зіставлення шаблонів, який використовує попередньо визначені або шаблони з параметрами обличь для визначення місцезнаходження чи виявлення обличь шляхом порівняння їх із вхідними фотографіями. Наприклад, обличчя людини можна розділити на чотири частини: очі, контур обличчя, ніс і губи. Крім того, використовуючи підхід виявлення країв, модель обличчя може бути побудована повністю з країв.

Хоча цей метод простий у розробці, його недостатньо для виявлення обличчя. Деформовані шаблони, з іншого боку, були представлені як рішення цих проблем.

Зіставлення шаблонів — це техніка, яка використовується для пошуку збігів між двома шаблонами.

На основі зовнішнього вигляду. Техніка, заснована на зовнішньому вигляді, щоб виявити моделі обличчя, залежить від колекції фотографій облич делегатів для навчання. Підхід, заснований на зовнішньому вигляді, перевершує всі інші методи оцінки ефективності. Під час пошуку відповідних якостей на фотографіях обличчя методи, засновані на зовнішньому вигляді, залежать від методів статистичного аналізу та машинного навчання, щоб виявити важливі характеристики фотографій обличчя. Цей підхід також використовується для виділення рис обличчя з метою розпізнавання обличчя.

Після цього модель на основі зовнішнього вигляду далі підрозділяється на під методи для виявлення обличчя, які є такими:

- **На основі власних граней**. Розпізнавання обличь виконується за допомогою алгоритму Eigenface, який є способом ефективного моделювання обличь за допомогою аналізу основних компонентів.
- **На основі розподілу**. Шаблони обличчя можна визначити за допомогою таких методів, як PCA та дискримінант Фішера, які обидва базуються на розподілі ймовірностей. Існує навчений класифікатор, який правильно відрізняє екземпляри цільового класу шаблону від екземплярів класу шаблону фонового зображення у вхідному зображенні.
- **Нейронні мережі**. Нейронні мережі ефективно використовувалися для вирішення широкого кола проблем виявлення, включаючи виявлення об’єктів, виявлення обличчя, виявлення емоцій та ідентифікацію обличчя, серед іншого.
- **Машина опорного вектора (SVM)**. Як лінійний класифікатор, опорні векторні машини (SVM) максимізують різницю в ймовірності між гіперплощиною рішення та кожним із екземплярів у навчальному наборі. Осуна та його колеги першими використали цей класифікатор для виявлення обличчя.
- **Розріджена мережа Winnows**. Було вирішено створити розріджену мережу, що складається з двох лінійних блоків або цільових вузлів; один представляє візерунки обличчя, а інший представляє візерунки без обличчя. Це менш трудомісткий і більш ефективний, ніж альтернатива.
- **Наївні байєсівські класифікатори**: Вони підрахували ймовірність того, що обличчя буде присутнім на фотографії, підрахувавши, скільки разів послідовність візерунка з’являлася в серії навчальних фотографій. Класифікатор зміг зібрати об’єднану статистику локального вигляду обличь та їх розташування на екрані.

- **Прихована модель Маркова**. Характеристики обличчя моделі будуть представлені станами моделі, які часто зображуються у вигляді смужок пікселів. HMM часто використовуються в поєднанні з іншими підходами для побудови систем виявлення.
- **Застосування теоретичних принципів інформації**. Випадкові поля Маркова (MRF) — це різновид випадкового поля, яке можна використовувати для аналізу малюнків обличчя та пов'язаних характеристик. Дивергенція Кульбака-Лейблера процесу Маркова використовується для максимізації розрізнення між класами в даних. У результаті ця технологія може бути використана для виявлення обличь.
- **Індуктивне навчання**. За допомогою цього методу було досягнуто визначення обличчя. Це досягається за допомогою використання таких алгоритмів, як C4.5 Квінлана або FIND-S Мітчелла.

2.3 Алгоритми розпізнавання обличчя.

Haar Cascades (2001). Детектор обличчя Віоли-Джонса, запропонований дослідниками Полом Віолою та Майклом Джонсом у 2001 році, став одним із перших великих проривів у цій галузі.

Використовуючи функції визначення ліній або країв, запропоновані в детекторі Віоли-Джонса, каскади Хаара (рис. 2.1) забезпечили вкрай необхідний прорив у розпізнаванні обличчя. Незважаючи на те, що це значно покращило швидкість і точність виявлення, воно мало свої обмеження та виявило невдачу, коли його викликали для виявлення облич у шумних зображеннях. За ці роки було багато покращень. Алгоритм Haar Cascade використовувався не лише для розпізнавання обличчя, але й для розпізнавання очей, розпізнавання номерних знаків тощо.

Класифікатор дивиться на інтенсивність пікселів і намагається знайти кілька попередньо визначених функцій на зображенні. Якщо він знаходить достатньо збігів для певного регіону, він може бути впевнений, що об'єкт є.

Підхід цих каскадів передбачає встановлення координат X, Y, Z та визначення ширини та висоти області для побудови прямокутної рамки на зображенні для ідентифікації необхідних областей. Завдяки стандартному розміру цих прямокутників, встановленому на рівні 24x24 пікселів, алгоритм демонструє здатність розрізняти приголомшливий масив із 162 000 унікальних візерунків. Тим не менш, це масштабне обчислення та аналіз може забрати багато часу. Щоб вирішити цю проблему, алгоритм Віоли-Джонса використовує модифіковану ітерацію навчального алгоритму AdaBoost для створення цих каскадів і ретельної оптимізації класифікаторів.

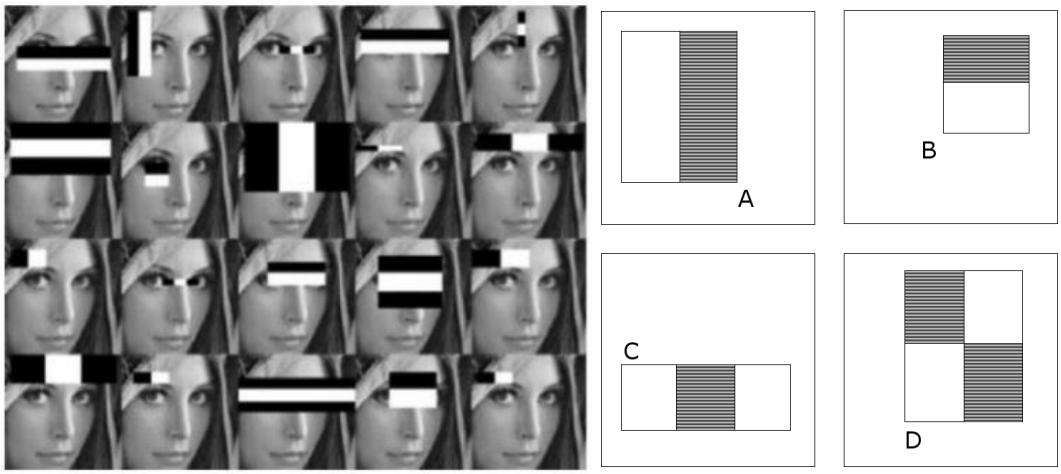


Рис. 2.1 Каскади Хаара.

Dlib-HOG (Histogram of Gradients) (2005). Надійний і сучасний метод відомий як гістограми орієнтованих градієнтів (HOG). Цей метод призначений для роботи з зображеннями в градаціях сірого. Алгоритм працює шляхом систематичного аналізу кожного пікселя, насамперед оцінюючи його відносну темність порівняно з сусідніми пікселями. Щоразу, коли сусідній піксель виявляється темнішим за той, що аналізується, стрілка позначається в напрямку темнішого пікселя, як показано на рисунку 2.2. Dlib використовує 5 фільтрів HOG: спереду, зліва, справа, , спереду, але повернуто ліворуч, спереду, але повернуто праворуч.

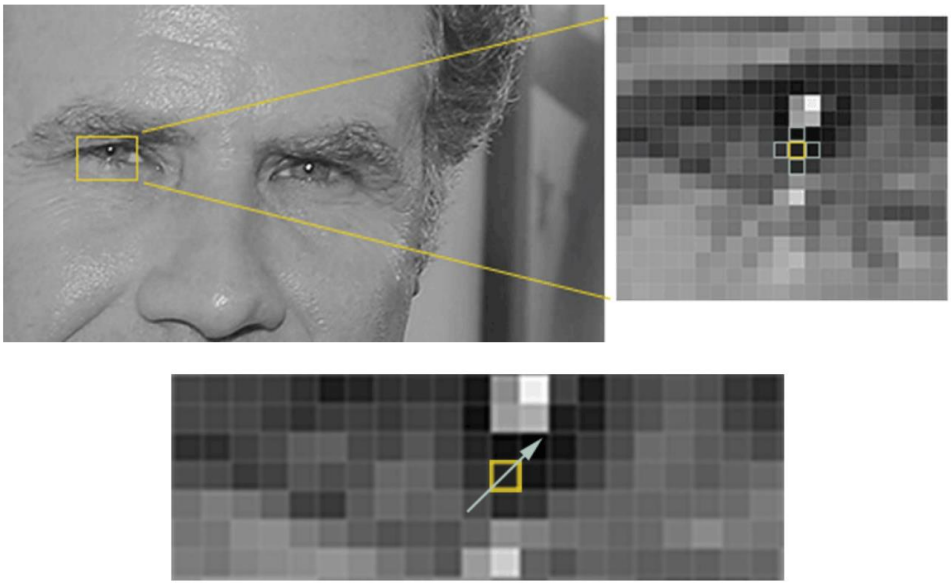


Рис. 2.2 Процедура оцінки окремого пікселя порівняно з його сусідніми.

Після застосування цього процесу до кожного пікселя зображення кожен піксель буде представлено стрілкою. Ці стрілки, відомі як градієнти, вказують напрямок переходу від світлого до темного зображення. Однак метою є підкреслити основні характеристики обличчя, що потребує сегментації зображення на блоки 16x16 пікселів. У кожному з цих блоків обчислюється кількість стрілок градієнта, що вказують у різних основних напрямках (що представляють різні напрямки, наприклад вгору, вниз, ліворуч, праворуч, верхній лівий, нижній лівий тощо). Згодом цей аналізований блок замінюється однією стрілкою, яка вказує на домінуючий напрямок у блоці. Зрештою вихідне зображення перетворюється на спрощене представлення, що забезпечує базовий структурний контур обличчя, як показано на рисунку 2.3.

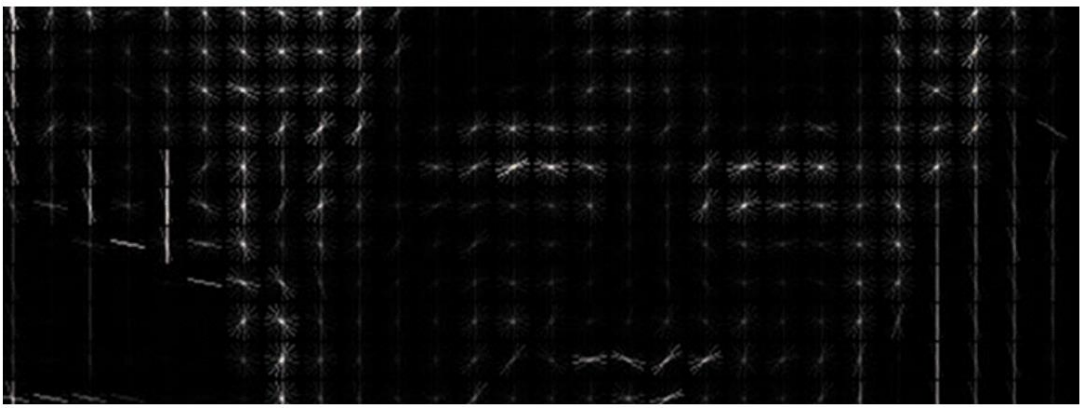


Рис. 2.3 Процедура поділу зображення на блоки 16x16 пікселів і визначення напрямків градієнта

MTCNN (2016). Більш сучасну модель, відому як MTCNN (див. рис. 2.4), що розшифровується як Multi-Task Cascaded Convolutional Neural Network, представили Zhang et al. У 2016 р. Ця широко поширена модель структурована як каскад взаємопов’язаних нейронних мереж. Архітектура MTCNN складається з трьох етапів згорткових нейронних мереж (CNN). На початковому етапі, відомому як P-Net (Мережа пропозицій), він швидко генерує вікна-кандидати за допомогою відносно простого CNN. Згодом стадія R-Net (уточнення мережі) ще більше покращує ці вікна, відкидаючи численні обмежувальні прямокутники без обличчя, використовуючи складнішу CNN. Нарешті, на етапі O-Net (Output Network) використовується потужніший CNN для подальшого уточнення результатів і визначення положення п’яти орієнтирів обличчя.

Хоча ця модель забезпечує високу точність, вона може бути непридатною для додатків у режимі реального часу через обмеження швидкості обробки.

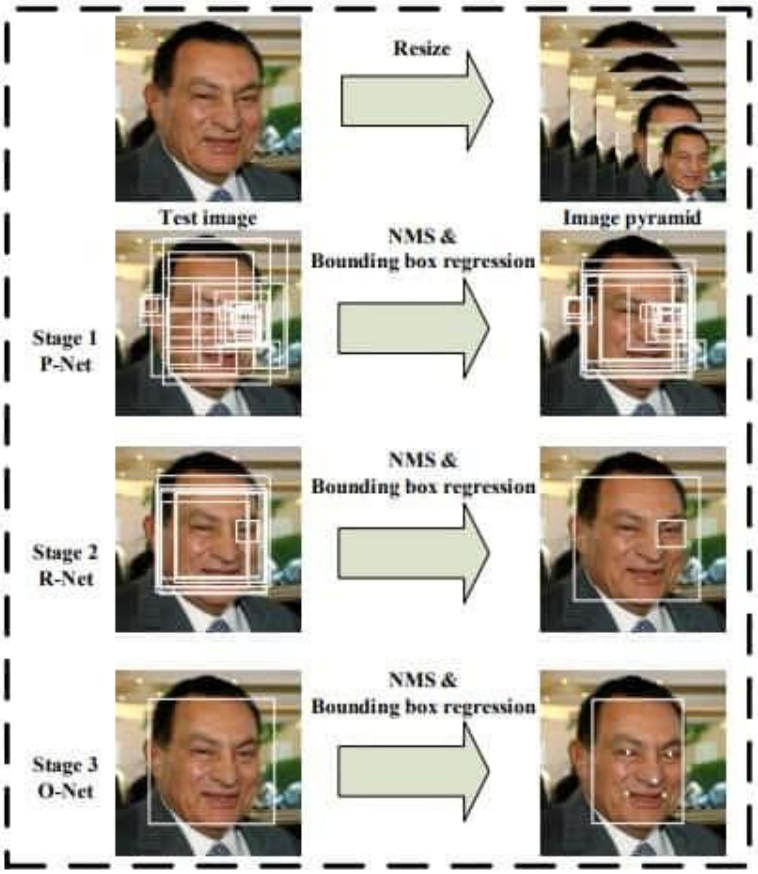


Рис. 2.4 Принцип роботи нейронної мережі MTCNN

У 2014 році Вахід Кеземі та Джозефін Салліван розробили алгоритм, відомий як «оцінка антропометричних точок» [7]. Цей метод призначений для

виділення 68 конкретних точок або міток на обличчі суб’єкта. До цих точок можуть входити характеристичні риси, такі як виступаюча частина підборіддя, контури очей, внутрішні межі брів та інші характерні особливості (див. рис. 2.4). Машина навчається розпізнавати ці специфічні мітки на обличчі кожної особи.

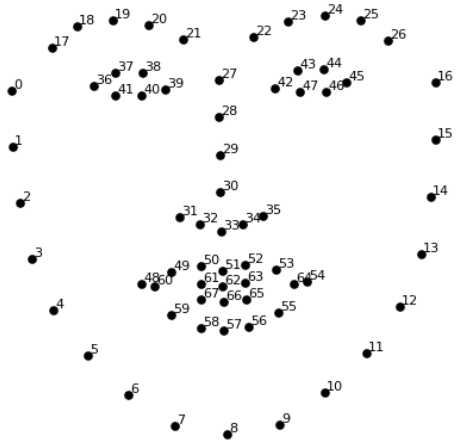


Рис. 2.5 – Перелік 68 спеціальних міток.

Тепер, використовуючи цей метод, машина може вирівняти моделі очей і рота, щоб вони розташовувалися приблизно в одному місці на зображенні. Це вдосконалення підвищує точність ідентифікації людини, зокрема визначення особи людини на фото чи відео. Цей етап часто виконується за допомогою штучної нейронної мережі. Це означає, що ми навчимо нашу мережу відрізняти конкретну людину від групи інших. Однак дуже важливо зрозуміти концепцію штучної нейронної мережі.

Штучна нейронна мережа (ШНМ) — це мережа взаємопов’язаних вузлів, яка нагадує структуру людського мозку (див. рис. 2.6). Ці мережі вивчають завдання, поетапно покращуючи свою функціональність на основі наданих їм прикладів. Наприклад, при розпізнаванні зображень тварин, наприклад кішок, системі надаються зображення кішок для аналізу.

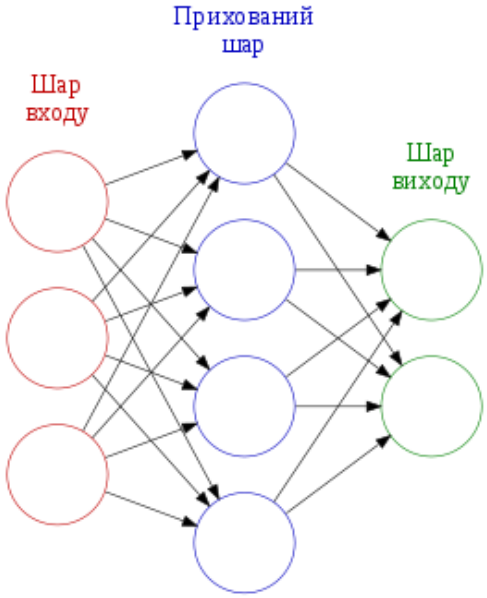


Рис. 2.6 Нейронна мережа, її вигляд

У нашому конкретному контексті процес розпізнавання обличчя включає злиття згорткових нейронних мереж (CNN). CNN представляють собою підтип мереж глибокого прямого зв'язку, що охоплює один або більше згорткових рівнів, за якими безперешкодно йдуть повністю пов'язані рівні штучної нейронної мережі (ANM). Ця форма глибокого навчання демонструє свою чудову здатність окреслювати важливі риси обличчя з більшою ефективністю, ніж люди-спостерігачі.

Щоб прискорити процедуру розпізнавання обличчя, глибока згорточна нейронна мережа генерує унікальний набір із 128 характеристик для кожної людини (як показано на рисунку 2.7). Цей інноваційний підхід, спочатку запропонований дослідниками Google у 2015 році, експерти з машинного навчання зазвичай називають персоналізованим набором функцій. Ці ознаки по суті представлені як масив числових значень, які обчислюються самою нейронною мережею та служать основою для подальшого аналізу та ідентифікації обличчя. У випадках, коли числові значення, отримані з двох зображень обличчя, дуже збігаються з мінімальним відхиленням, ці два обличчя з упевненістю класифікуються як ідентичні.

Рис. 2.7 Вигляд 128 унікальних особливостей особи

Під час навчання використовуються фотографії, які користувач завантажує в систему. Що більше фотографій доступно для навчання, тим точніше і акуратніше буде аналіз та результати ідентифікації.

2.4 Характеристики нейронної мережі MobileNet

Мова заговорила про нейронні мережі, тож давайте розглянемо конкретні моделі, які впроваджуються у нашому програмному модулі. Першою важливою нейронною мережею є MobileNet. Ця модель базується на спрощеній архітектурі та використовує роздільні згортки за глибиною для створення легких CNN (згорткових нейронних мереж). Нейронна мережа MobileNet є високоефективною моделлю, особливо в контексті мобільних та вбудованих застосувань комп’ютерного зору. Вона знаходить широке застосування у реальних програмах, включаючи виявлення об’єктів, деталізовану класифікацію, аналіз обличчя та точну локалізацію.

Роздільні згортки за глибиною включають два етапи:

- Згортка по глибині (глибинна згортка).
- Точкова згортка.

Зазвичай, перший шар використовується для фільтрування вхідних каналів, тоді як другий шар поєднує їх для створення нової характеристики. Давайте для початку розглянемо, що означає звичайна операція згортки.

В звичайній операції згортки використовується вхідне зображення розміром N на N з N_C каналами, де

- N_C – це кількість каналів,
- N – це кількість пікселів на зображенні.

Для ілюстрації, давайте візьмемо зображення із трьома каналами, кожен з них має розмір 6 на 6 пікселів. Далі ми спробуємо здійснити операцію згортки за допомогою фільтра F розміром $FxFxN_C$, який в розрахунках буде представлений як тривимірний блок розміром 3x3x3. Операція згортки зменшить розмір вихідних значень до 4 на 4. Для заповнення цієї операції згортки нам потрібно пройтися кроком в одиницю (див. рис. 2.8). Всього на кожному етапі застосування фільтра ми виконуємо 27 множень, які потім підсумовуються і внесені до першого блоку значень розміром 4 на 4. Кількість каналів у вихідному результаті залежить від кількості самі фільтрів. Тобто, якщо ми використовуємо 5 фільтрів розміром 3 на 3 на 3, то вихід матиме розмірність 4 на 4 на 5.

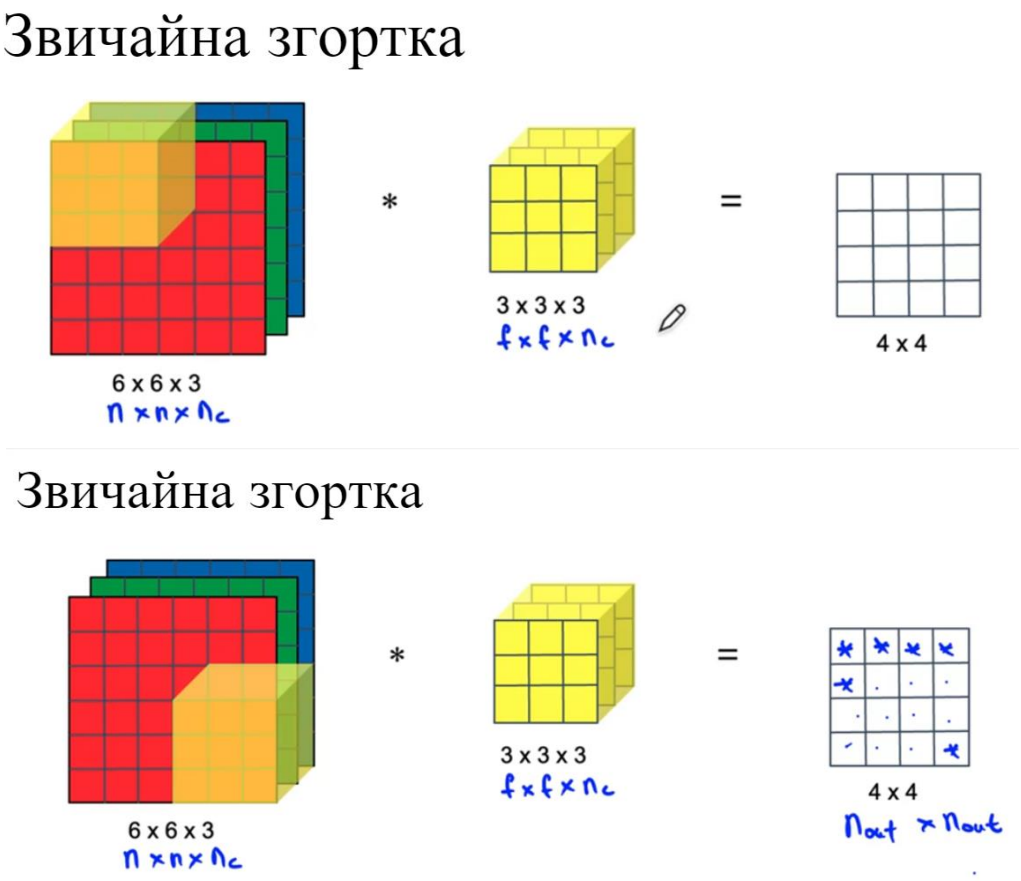


Рис. 2.8 Процес проходження фільтру (3 на 3 на 3) з кроком в один (1) по вхідному зображенню.

Давайте визначимо обчислювальну складність операції, яку ми щойно виконали. У нашому випадку параметри фільтра 3x3x3, позиції фільтра відповідають кількості можливих місць для розміщення фільтра, тобто 4x4, і ми маємо 5 фільтрів. Таким чином, загальна вартість обчислень розраховується за такою формулою:

$$\text{Вартість} = n \text{ параметрів} * n \text{ позицій} * n \text{ фільтрів} \quad (2.1)$$

Отже, виходячи з нашого прикладу:

$$\text{Вартість} = (3 * 3 * 3) * (4 * 4) * 5 = 2160.$$

Тепер давайте звернемо нашу увагу на згортку, що розділяється по глибині, яка є фундаментальним компонентом нашої нейронної мережі MobileNet. Цей метод нагадує стандартну згортку, але містить кілька важливих нюансів. Роздільна згортка по глибині ґрунтується на двоетапному процесі (див. рис. 2.9).

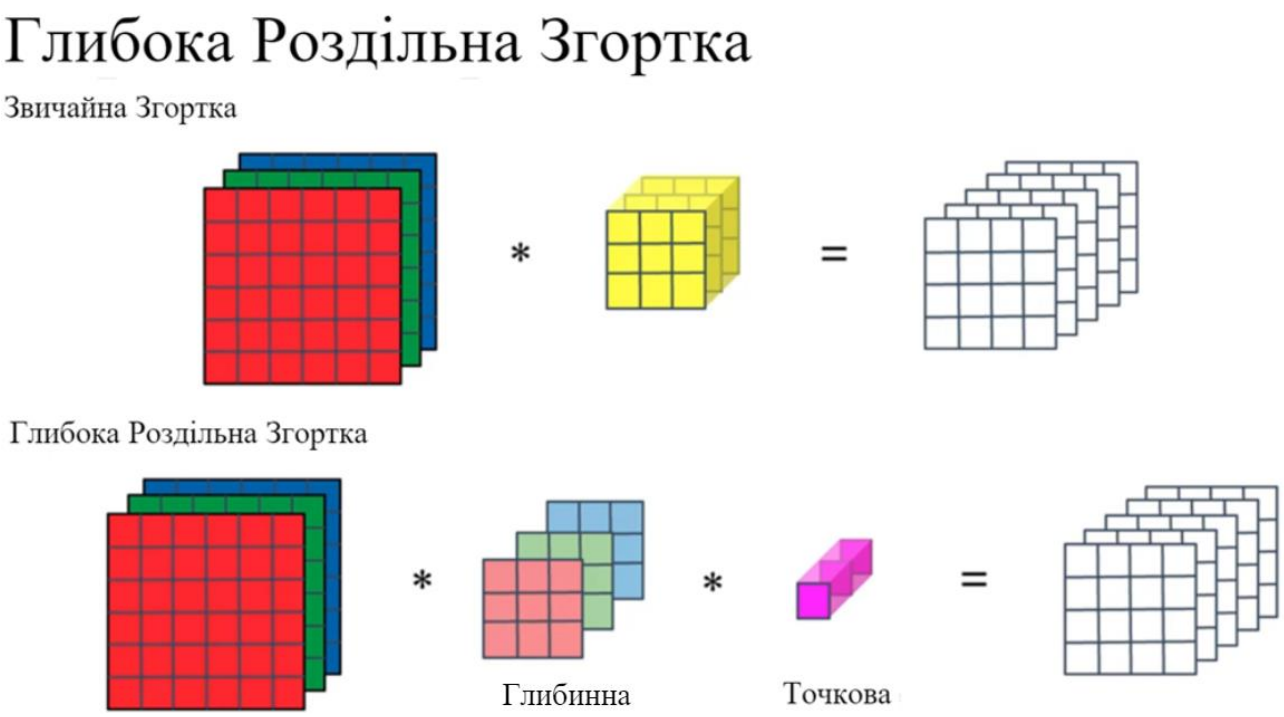


Рис. 2.9 Звичайна Згортка. Глибинна Роздільна Згортка. Показ їх структур.

Перший етап стосується глибинної згортки. Розглянемо, як працює цей метод. Ми починаємо з того самого зображення з трьома (3) каналами, а також розміром 6x6 пікселів кожен, тобто N x N x N_C. До цього зображення ми застосовуємо фільтр із розмірами F x F. Тут починаються перші зміни. У нашому сценарії кількість фільтрів дорівнює NC, тобто 3. Підхід для обчислення вихідних даних 4x4x3 передбачає застосування одного фільтра до одного

вхідного каналу відповідно (див. рис. 2.10). По суті, ми запускаємо кожен відповідний фільтр через кожен відповідний вхідний канал.

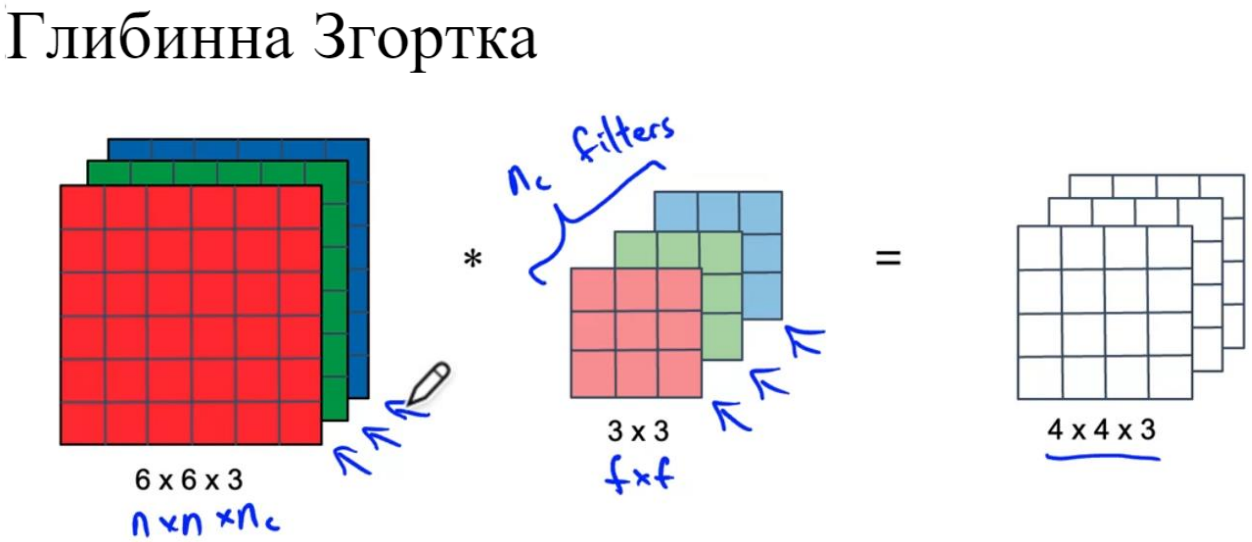


Рис. 2.10 Згортка по глибині. Відповідність фільтрів да вхідних каналів зображення.

Давайте в якості прикладу розглянемо перший червоний фільтр. Оскільки ми беремо лише один фільтр (червоний) розміром FxF, ми проводимо лише 9 операцій множення, що виявляється менше, ніж 27, як це було у звичайній згортці. Під час обчислення, коли ми накладаємо фільтр на першу область зображення, ми записуємо інформацію в перший блок згортки розміром 4x4 (див. рисунок 2.11). У нашому випадку, з розміром фільтру 3x3 та зображенням 6x6, ми можемо виконати цю процедуру 4x4 рази, оскільки ми проходимо через повністю весь червоний канал зображення з діапазоном зсуву в одиницю. Розмір виходу матиме вигляд N_{out} x N_{out} x N_C, де:

- N_C – це кількість каналів вхідного фото,
- N_{out} – кількість вихідних пікселів.

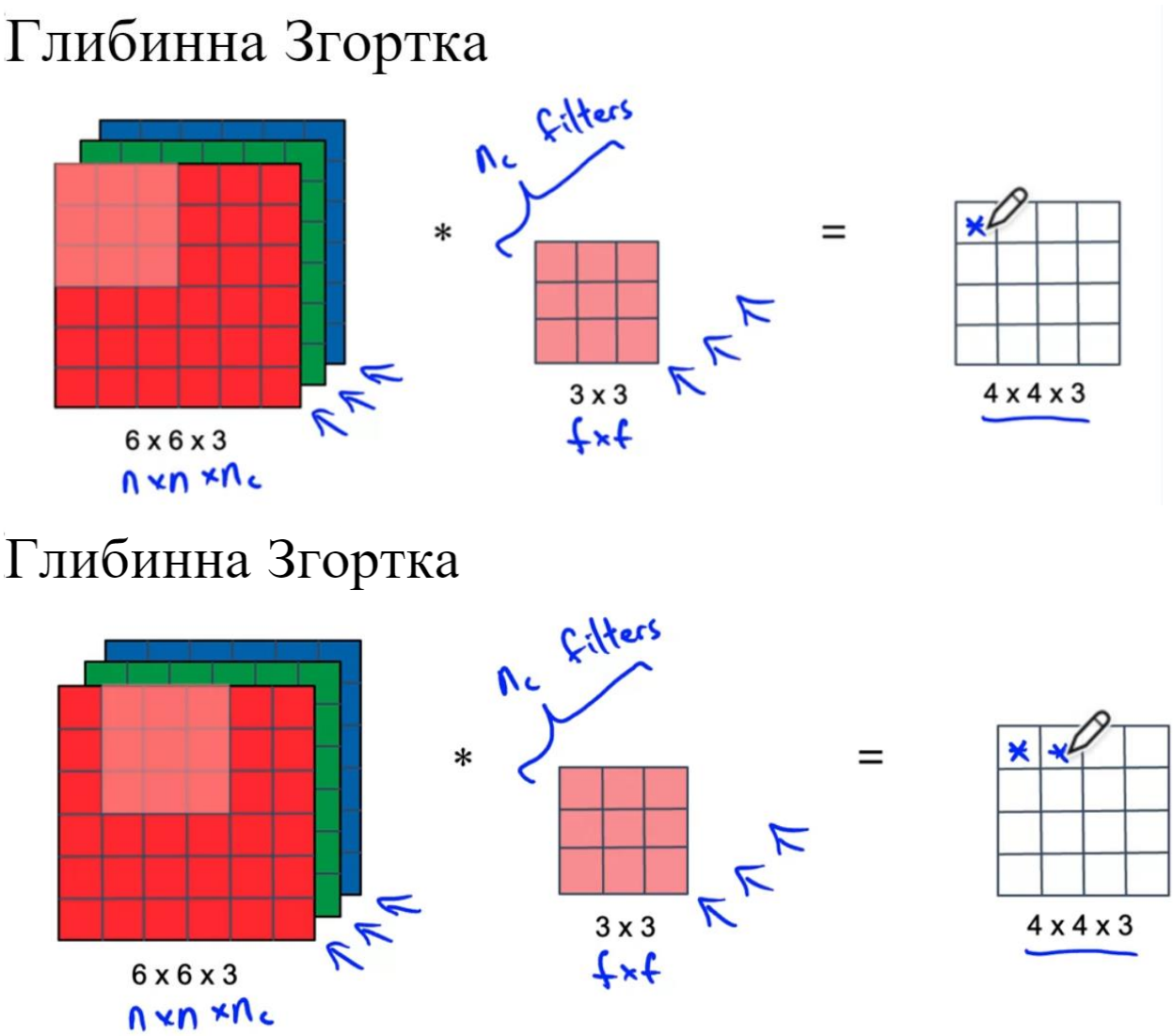


Рис. 2.11 Проходження фільтру з діапазоном зсуву в одиницю по вхідному каналу зображення.

Тепер давайте дослідимо обчислювальну складність процедури, яку ми щойно виконали. Подібно до звичайної згортки (2.1), формула демонструє значну схожість. Однак у випадку поглибленої згортки кількість параметрів фільтра позначається як FxF, а не $FxFxN_C$. Отже, кожен фільтр потребує загалом 9 (3x3) множень. Кількість позицій залишається незмінною, з 16 можливими позиціями фільтра для сканування зображення з кроком 1. Кількість фільтрів залежить від каналів, присутніх у вхідне зображення, яке в нашому прикладі складається з 3 каналів (червоний, зелений, синій). Кінцева обчислювальна вартість цієї операції може бути виражена як:

$$\text{Вартість} = n \text{ параметрів} * n \text{ позицій} * n \text{ фільтрів}$$

$$432 = (3*3) * (4*4) * 3$$

Однак це лише початковий крок у нашому процесі згортання по глибині. Після отримання виходу з першої фази, яка відповідає глибинній згортці, ми переходимо до наступної фази – точкової згортки. Щоб виконати точкову згортку, обов'язково потрібно вибрати проміжне значення, отримане з поглибленої згортки, яка в цьому контексті має розміри 4x4x3. Згодом до цього проміжного значення застосовується точкова згортка, що дає результат 4x4x5, як показано на рисунку 2.12.

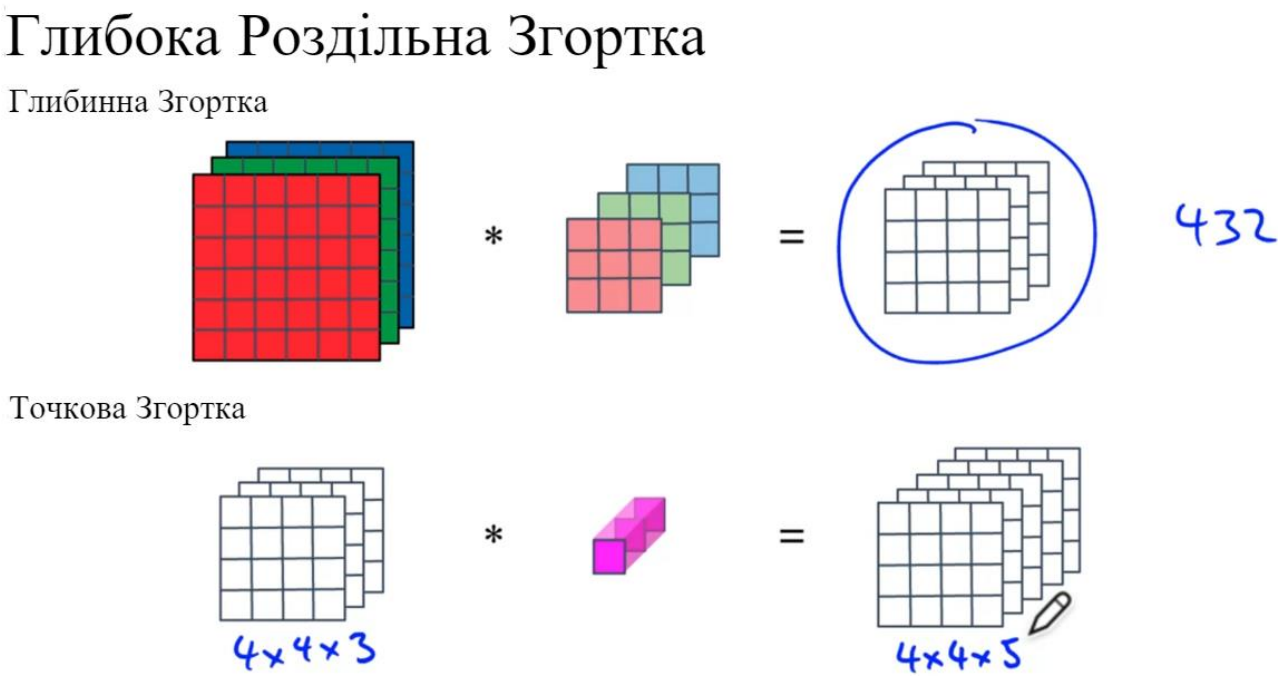


Рис. 2.11 Результат глибинної згортки та перехід до точкової згортки.

Використовуючи проміжну колекцію значень глибини згортки, позначених як $N_{out}xN_{out}xN_C$, ми використовуємо блок $1x1xN_C$ у кожній позиції, як показано на рисунку 2.11. Це передбачає три множення для кожної позиції з подальшим підсумовуванням цих результатів і включенням результату у відповідний блок вихідного значення. Згодом ми переходимо до всіх 16 позицій у проміжному наборі вхідних значень, як показано на рисунку 2.12. Цей процес виконується лише за допомогою одного фільтра. Щоб отримати додатковий вихід 4x4, що становить розмірні виходи 4x4x5, ми повинні відтворити цю процедуру з фільтрами N_C, що в нашому конкретному сценарії становить 5 фільтрів. По суті, це вимагає застосування цієї процедури з чотирма додатковими фільтрами.

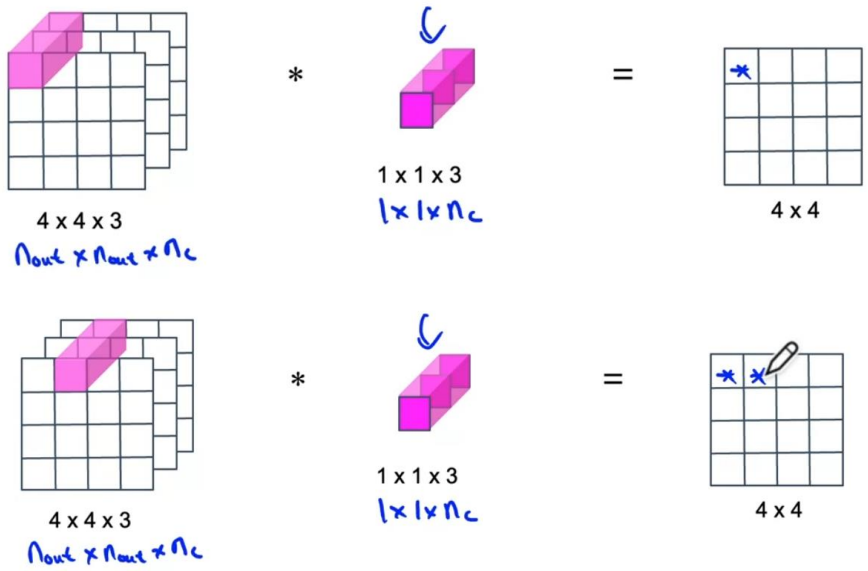


Рис. 2.12 Проходження точкового фільтру з діапазоном зсуву в одиницю.

Давайте повернемося до обчислювальної вартості операцій, які ми щойно виконали. Для кожного з вихідних значень 4x4x5 ми застосували рожевий фільтр до ділянки вхідних даних. Це включало три операції, що відповідає фільтру 1x1x3, який представляє n-параметрів фільтра. Позиції фільтра з параметрами 1x1x3 можна розташувати в межах глибини введення 4x4x3. Для досягнення глибокої роздільної згортки ми використовували 5 фільтрів. Отже, виходячи з наведеної вище інформації, остаточну формулу можна виразити наступним чином:

$$\text{Вартість} = n \text{ параметрів} * n \text{ позицій} * n \text{ фільтрів}$$

$$240 = (1 * 1 * 3) * (4 * 4) * 5$$

Отже, загальна кількість множень на цій стадії згортки становить 240.

На прикладі, який розглянули раніше, звичайна згортка обробляла вхідні значення 6x6x3, що призвело до виходу 4x4x5. Те саме стосується згортки з роздільною глибиною, за винятком того, що ми виконали її в два кроки: згортка в глибину, за якою йде згортка по точках. Якою була обчислювальна вартість усіх цих операцій? У випадку стандартної згортки нам довелося зробити 2160 множень для отримання результату. Для згортки з роздільною глибиною було 432 множення на кроці глибини та 240 множень на кроці поточкової згортки, що підсумовує 672 множення. А тепер, якщо ми обчислимо співвідношення між

цими числами (672 та 2160), ми отримаємо приблизно 0,31. Як видно, результат значно нижчий за розрахункову вартість.

Архітектура MobileNet вводить два гіперпараметри: множник ширини та множник глибини, також відомий як «множник роздільної здатності». Множник ширини визначає кількість каналів у кожному шарі зображення. Ці два параметри забезпечують гнучкість налаштування розміру мережі. Зменшення ширини та глибини може знизити точність розпізнавання, але це підвищує швидкість роботи та зменшує споживання пам’яті.

2.4 Особливості нейронної мережі SSD

Single Shot Detector (SSD) є частиною сімейства методів виявлення об’єктів «поодинокого пострілу», що означає, що він може миттєво ідентифікувати всі можливі об’єкти на зображенні. Існує ще одна відома нейронна мережа під назвою «You Only Look Once» (YOLO), але ми зосередимося на SSD, оскільки він більш сучасний і кращий. SSD стане основою для нашого програмного модуля для виявлення об’єктів різних розмірів.

Підхід SSD передбачає дискретизацію вихідного простору прямокутників у набір стандартних квадратів із різними пропорціями та масштабами, розміщених на карті функцій. Під час фази передбачення мережа виробляє оцінки присутності кожних видів об’єктів у цих вікнах за замовчуванням і вносить коригування, щоб більш точніше відповідати формі та положенню об’єктів.

Крім того, мережа SSD об’єднує прогнози з декількох карт функцій з різноманітною роздільною здатністю, щоб як найприродніше розмістити об’єкти різних розмірів. На відміну від методів, які передбачають генерацію пропозиції об’єкта, модель SSD спрощує процес, усуваючи необхідність генерації пропозиції та подальших кроків повторної дискретизації пікселів або функцій. Він інкапсулює обчислення в одній єдиній мережі, полегшуючи навчання та інтеграцію в підсистеми, які потребують виявлення об’єктів.

Експериментальні результати на таких наборах даних, як «PASCAL VOC», «MS COCO» та «ILSVRC», підтверджують, що SSD досягає точності, порівнянної з методами, які експлуатують додаткові етапи пропозиції об’єктів, але працюють набагато швидше. Він забезпечує єдину структуру як для навчання, так і для висновків. Навіть з маленьким розміром вхідного зображення, SSD перевершує інші одноетапні методи з точки зору точності.

Підхід SSD побудований на методі прямої згорткової мережі, яка генерує обмежувальні прямокутники фіксованого розміру та оцінює наявність екземплярів класу функцій у цих коробках. Потім застосовується немаксимальний етап придушення для отримання остаточних виявлень. Початкові рівні мережі базуються на стандартній архітектурі для класифікації високоякісних зображень, яка називається базовою мережею. Мережа оснащена системою підтримки виявлення, яка включає такі ключові функції.

Тепер давайте розберемося, як працює ця система. Він починається із зображення відповідного розміру в пікселях. Серія згорткових шарів застосовується до зображення, поступово зменшуючи його просторові розміри до 1x1 пікселів. Для кожного з цих шарів додається відповідний блок виявлення. Це гарантує, що нейронна мережа може ефективно виявляти об’єкти різного розміру на зображенні. На кожному масштабі розміщуються рамки для захоплення об’єктів, що охоплюють зображення в різних масштабах. Згодом багато з цих блоків фільтруються, а вихід детектора об’єктів виробляється шляхом об’єднання всіх шарів. Цей процес показано на рисунку 2.13.

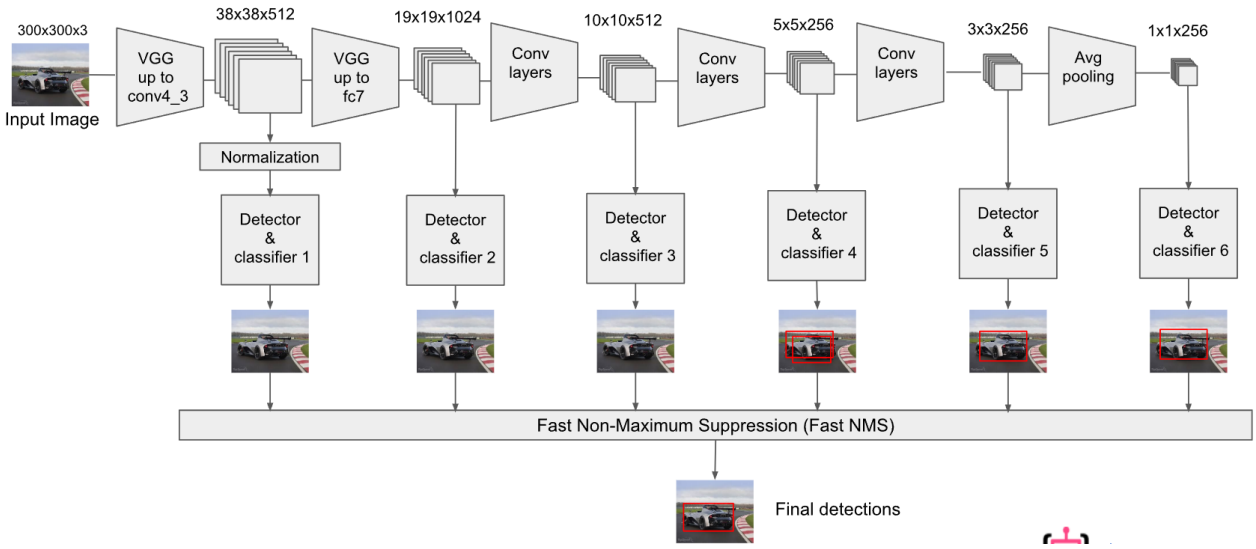


Рис. 2.13 Накладання згорткових шарів на зображення, а потім додавання блоків детектора для детектування об’єктів різних розмірів.

Тепер давайте глибше заглибимося в структуру та функціональність цих блоків, які вводяться після накладання згорткових шарів (див. рис. 2.14). Ці блоки включають:

- Створення спеціальних блоків, відомих як стандартні блоки (default boxes).
- Застосування стандартної згортки 3x3 для налаштування цих спеціальних полів (default boxes).
- Використання іншої стандартної згортки 3x3 для класифікації скоригованих блоків, що виконується після вищезгаданих операцій.

Нехай в нас будуть задані наступні параметри:

- Розмір вхідного зображення (300 x 300)
- Розмір сітки (feature maps) (5 x 5 x 256)
- Кількість спеціальних боксів (default boxes) = 3

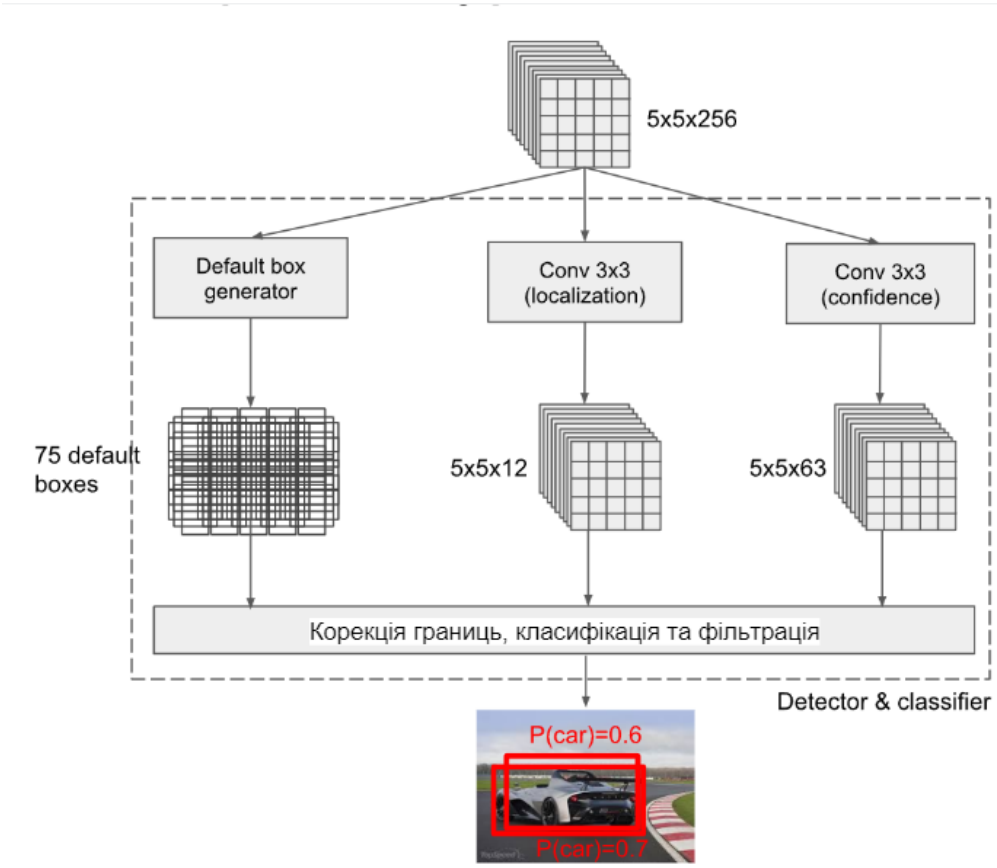


Рис. 2.14 Показ архітектури блоку «Detector» та «Classifier».

Тепер давайте розглянемо процес генерування спеціальних блоків, також відомих як блоки за замовчуванням. Ці коробки генеруються шляхом створення сітки, і розмір цієї сітки залежить від масштабу. У цьому прикладі (див. рис. 2.15) сітка має розмір 5x5, а червоні точки представляють центри цих прямокутників. Ці поля разом охоплюють все зображення, причому кожна клітинка сітки відповідає трьом полям за замовчуванням. Кожен із цих спеціальних прямокутників визначається координатами центру, висотою та шириною. Параметри системи визначають розміри цих ящиків.

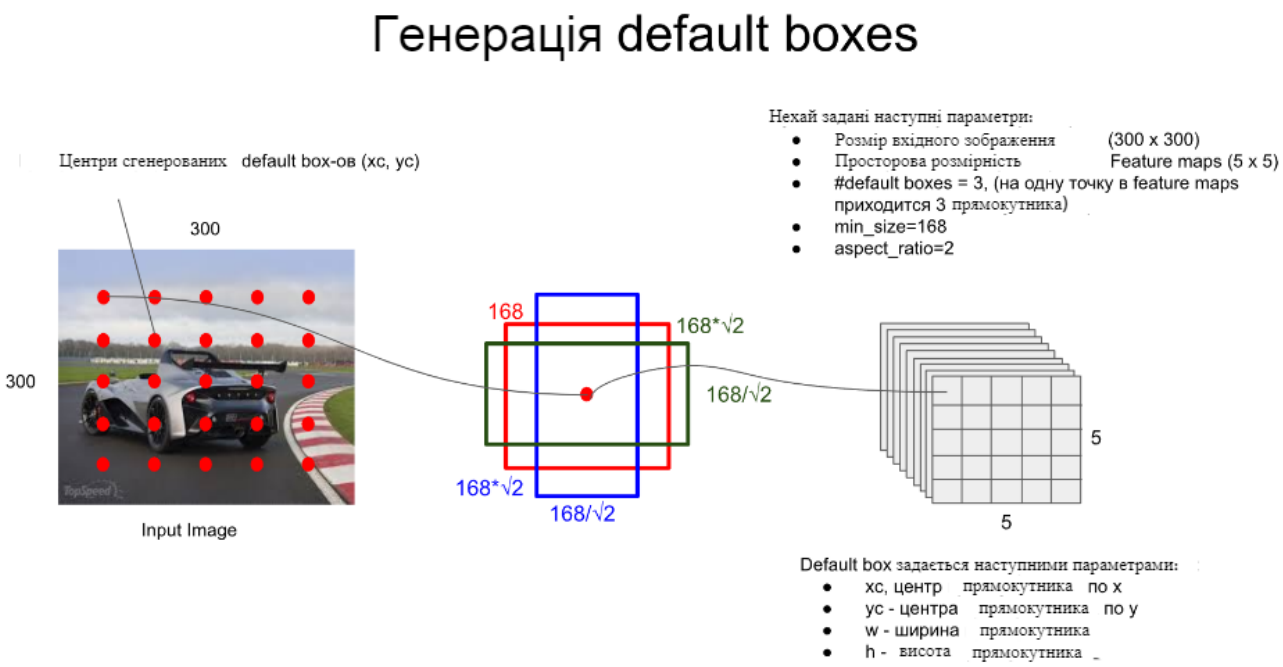


Рис. 2.15 Генерація спеціальних блоків (боксів) для виявлення об’єктів

Генерація цих коробок призводить до загалом 5x5x3 коробок, що означає сітку 5x5 із 3 коробками в кожній клітинці, що становить 75 коробок у цьому блоці. Ці поля разом охоплюють все зображення, а потім фільтруються, локалізуються за допомогою шарів і обробляються мережею.

SSD має склад з двох основних компонентів: базової моделі та головки SSD. Базовою моделлю зазвичай є попередньо навчена мережа класифікації зображень, яка використовується як екстрактор ознак. Загальним вибором є мережа на кшталт ResNet, яка навчена за допомогою ImageNet, з видаленим остаточним повним шаром класифікації. Ця установка дає глибоку нейронну мережу, здатну витягувати семантичну інформацію з зображення, зберігаючи при цьому структуру зображення, хоча й із зниженою роздільною здатністю.

2.5 Висновки до другого розділу

Виходячи з проаналізованої інформації у другому розділі кваліфікаційної роботи було встановлено технологію комп’ютерного зору разом з машинним навчанням. Розглянуто питання їх взаємодії, методами роботи, алгоритми та логіку експлуатації.

Сфера алгоритмів розпізнавання обличь зазнала значного прогресу за ці роки. У цьому розділі дисертації розглядається історичний розвиток цих алгоритмів, починаючи з піонерського методу Пола Віоли та Майкла Джонса, який використовував функції Хаара та технологію AdaBoost. Він також висвітлює більш сучасні та універсальні алгоритми розпізнавання, такі як ті, що використовують гістограму орієнтованих градієнтів (HOG). Обговорюється концепція використання 68 орієнтирів обличчя або точок як еталонних міток для збереження певної області обличчя в центрі зображення, що відображає постійну еволюцію методів розпізнавання обличчя.

Крім того, досліджується інтеграція штучних нейронних мереж в аналіз обличчя, що проливає світло на виняткову швидкість і ефективність глибокої нейронної мережі MobileNet. Експертиза розрізняє три типи згорток, залучених до роботи нейронної мережі, підкреслюючи їх значення в аналізі зображень.

Штучна нейронна мережа SSD (Single Shot Detector) представлена як багатообіцяючий прорив у сфері комп’ютерного зору, із застосуваннями, починаючи від виявлення об’єктів до розпізнавання. Розділ пропонує розуміння принципів роботи нейронної мережі SSD.

Як було з’ясовано, ідентифікація обличчя здійснюється за допомогою синергічного застосування нейронних мереж і спеціалізованих баз даних, що містять біометричні риси обличчя. Варто відзначити, що подібні методи ідентифікації використовують різні біометричні характеристики, такі як форма вуха, структура долоні або малюнок вен.

Синтез цих різних методів і підходів підкреслює безперервний прогрес технологій розпізнавання обличчя, що має ширші наслідки для безпеки, автоматизації та ідентифікації в різних областях. Таке поєднання методології прокладає шлях до більш ефективних, точних і безпечних систем розпізнавання.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОГРАМНОГО МОДУЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА

3.1. Вибір технологій та середовища обробки.

Середовище розробки Visual Studio: інтегроване середовище розробки для сучасної розробки програмного забезпечення.

Код Visual Studio, який часто називають VS Code, є популярним і універсальним інтегрованим середовищем розробки (IDE), розробленим Microsoft. Він отримав широке визнання та прийняття в спільноті розробників програмного забезпечення завдяки широкому набору функцій, крос-платформній сумісності та підтримці великої екосистеми розширень. У цьому дипломі ми досліджуватимемо різні аспекти VS Code, його історію, особливості та значення в сучасній розробці програмного забезпечення.

Visual Studio Code був спочатку випущений у квітні 2015 року. Він виник у результаті бажання Microsoft створити легкий редактор коду з можливістю налаштування, який міг би задовольнити різноманітні потреби розробників. Розроблений з використанням Electron, фреймворку для створення кросплатформних програм, він сумісний із Windows, macOS і Linux, забезпечуючи узгоджену роботу для розробників на різних платформах.

VS Code пропонує безліч функцій, які покращують продуктивність розробника та покращують досвід кодування. Серед важливих особливостей:

- Інтелектуальне редагування коду: VS Code надає такі функції, як підсвічування синтаксису, автозавершення та навігація коду, щоб допомогти розробникам писати код ефективно.
- Інтеграція контролю версій: він легко інтегрується з такими популярними системами контролю версій, як Git, дозволяючи розробникам керувати та відстежувати зміни у своїй кодовій базі.
- Розширення: одним із найпотужніших аспектів VS Code є його система розширення. Розробники можуть встановлювати розширення, щоб

додавати нові мови, теми або спеціальні функції, щоб адаптувати IDE до своїх конкретних потреб.

- Налагодження: VS Code пропонує надійні можливості налагодження з підтримкою різних мов і середовищ виконання.
- Інтегрований термінал: містить вбудований термінал, що усуває необхідність перемикатися між IDE та зовнішніми термінальними програмами.
- Автоматизація завдань: розробники можуть створювати та запускати завдання та створювати процеси безпосередньо в VS Code.
- Кросплатформна розробка: VS Code є чудовим вибором для веб- та хмарної розробки, що підтримує такі технології, як JavaScript, TypeScript, Node.js тощо.
- Live Share: функція Live Share забезпечує співпрацю в реальному часі, дозволяючи кільком розробникам одночасно працювати над однією кодовою базою.

Ринок розширень для VS Code великий, з тисячами доступних розширень для різних мов програмування та інструментів. Ця можливість розширення дозволяє розробникам налаштовувати свою IDE відповідно до потреб свого проекту. Ви можете знайти розширення для підтримки мови, лінінгування коду, інфраструктури тестування та багато іншого.

У Visual Studio Code є велика та активна спільнота розробників, які роблять внесок у його розробку та надають підтримку через форуми, документацію та онлайн-навчальні посібники. Залучення спільноти та постійне вдосконалення сприяють постійному успіху VS Code.

Visual Studio Code став універсальним і важливим інструментом для розробки сучасного програмного забезпечення. Його широкі можливості, кросплатформна сумісність і яскрава екосистема розширень роблять його кращим вибором для розробників у всьому світі. Незалежно від того, чи працюєте ви над веб-розробкою, мобільними додатками чи хмарними службами, VS Code пропонує потужне, настроюване та ефективне середовище для ваших проектів

програмування. Його зручний інтерфейс і безперервні оновлення гарантують, що він і надалі буде цінним надбанням для розробників програмного забезпечення протягом багатьох років.

В умовах веб-розробки, що постійно змінюється, дуже важливо використовувати сучасні технології для створення привабливих і ефективних веб-додатків. Ми інтегруємо JavaScript, TypeScript, React з Redux Toolkit, HTML і CSS у процес розробки. Ці технології були використані в дипломному проекті, що призвело до створення надійної, зручної та багатофункціональної веб-програми.

JavaScript є основною мовою програмування для веб-розробки. Він забезпечує динамічні та інтерактивні функції у веб-додатках. У вашому дипломному проекті JavaScript відіграв ключову роль у:

- Інтерактивність: JavaScript дозволяє створювати динамічні інтерфейси користувача, уможливлюючи такі дії, як перевірка форм, оновлення в реальному часі та адаптивні елементи дизайну.
- Асинхронні операції: асинхронні можливості JavaScript були використані для отримання даних з API, забезпечуючи безперебійну взаємодію вашої програми із зовнішніми службами.
- Обробка подій: кероване подіями програмування в JavaScript полегшує взаємодію користувача, наприклад обробку клацань, натискань клавіш і рухів миші.

TypeScript — це статично типізований наднабір JavaScript, який додає до процесу розробки підтримку безпеки типів і інструментів. Його переваги у вашому проекті включали:

- Безпека типів: TypeScript допомагає виявляти помилки під час розробки, зменшуючи проблеми під час виконання та покращуючи якість коду.
- Супроводжуваність коду: надаючи чіткий та самодокументований код, TypeScript покращує придатність проекту, полегшуючи співпрацю членів команди.

- Розширена підтримка IDE: TypeScript пропонує кращу підтримку інструментів, включаючи автозаповнення коду, перевірку типу та інтелектуальний рефакторинг, покращуючи загальний досвід розробки.

React — це популярна бібліотека JavaScript для створення користувальницьких інтерфейсів, а Redux Toolkit — бібліотека для керування станом. Їх поєднання дає ряд переваг:

- Розробка на основі компонентів: React дозволяє створювати повторно використовувані компоненти, спрощуючи структуру проекту та сприяючи повторному використанню коду.
- Управління станом: Redux Toolkit забезпечує передбачувану систему керування станом, що полегшує керування та обмін даними між компонентами.
- Спрощене керування станом: Redux Toolkit спрощує налаштування та зменшує шаблонний код, оптимізуючи процес керування станом.
- Інструменти розробника: Інструменти розробника Redux Toolkit надають уявлення про стан і дії програми, сприяючи налагодженню та тестуванню.

HTML і CSS є основою веб-розробки, відповідальною за структурування вмісту та його стиль. У вашому проекті:

- HTML забезпечив структуру ваших веб-сторінок, визначивши елементи та їхні зв’язки в документі.
- CSS використовувався для стилізації, дизайну макета та забезпечення візуально привабливого інтерфейсу користувача.
- Адаптивний дизайн: медіа-запити CSS дозволили вашій програмі адаптуватися до різних розмірів екрана, забезпечуючи узгоджену взаємодію з користувачем на різних пристроях.
- Доступність: HTML використовувався з атрибутами ARIA та семантичними елементами, щоб зробити проект більш доступним для всіх користувачів.

Основним нашим фреймворком буде бібліотека Tensorflow.js. TensorFlow.js — це бібліотека JavaScript з відкритим вихідним кодом, яка дозволяє розробникам передавати потужність машинного навчання та моделей глибокого навчання у веб-додатки безпосередньо в браузері. У цьому розділі ми заглибимося в TensorFlow.js, його можливості та його значення в царині веб-машинного навчання.

TensorFlow.js, яку часто називають tf.js, — це бібліотека, яка розширює екосистему TensorFlow у домен JavaScript. Це дозволяє розробникам створювати та тренувати моделі машинного навчання, а також робити висновок у середовищі веб-браузера. Ця технологія об’єднує світи веб-розробки та машинного навчання, пропонуючи унікальну платформу для створення додатків на основі ШІ.

Основні характеристики та можливості:

- Машинне навчання на основі браузера: TensorFlow.js дозволяє розробляти моделі машинного навчання, які можна запускати безпосередньо у веб-браузері. Це усуває потребу в обчисленнях на стороні сервера та підвищує конфіденційність користувачів, зберігаючи дані на стороні клієнта.
- Простота використання: бібліотека розроблена з урахуванням зручності користувача, що робить її доступною як для веб-розробників, так і для практиків машинного навчання. Він надає API високого рівня для звичайних завдань, одночасно пропонуючи доступ нижчого рівня для більш складних випадків використання.
- Перетворення моделі: TensorFlow.js полегшує перетворення попередньо навчених моделей TensorFlow (часто на Python) у формат, сумісний з Інтернетом, що дозволяє використовувати існуючі моделі у веб-додатках.
- Передача навчання: розробники можуть використовувати передачу навчання шляхом точного налаштування попередньо підготовлених моделей на основі даних, що стосуються домену, зменшуючи потребу у великих наборах даних і тривалому навчанні.

- Виведення в реальному часі: TensorFlow.js оптимізовано для висновків у реальному часі, що робить його придатним для таких програм, як розпізнавання зображень і звуку, виявлення об’єктів, аналіз настроїв тощо.
- Апаратне прискорення: він підтримує апаратне прискорення за допомогою WebGL, що дає змогу ефективно запускати моделі на GPU, таким чином підвищуючи продуктивність.

TensorFlow.js знаходить застосування в різних областях, зокрема:

- Обробка зображень і відео: класифікація зображень у реальному часі, виявлення об’єктів і аналіз відео можна досягти за допомогою TensorFlow.js.
- Обробка природної мови (NLP): аналіз настроїв, генерація тексту та моделі перекладу мови можна реалізувати безпосередньо в браузері.
- Розпізнавання жестів: використовується для розробки систем розпізнавання жестів для інтерактивних веб-додатків.
- Навчальні інструменти: TensorFlow.js використовується для створення освітніх ресурсів, таких як інтерактивні посібники з машинного навчання.
- Пристрої IoT та Edge: легкий характер TensorFlow.js робить його придатним для пристроїв Edge та IoT, де обчислювальні ресурси обмежені.

Спільнота TensorFlow.js активна і постійно зростає. Він надає достатньо ресурсів, включаючи документацію, навчальні посібники та готові моделі. Інтеграція з TensorFlow, TensorFlow Hub і TensorFlow.js також відкриває світ попередньо навчених моделей і можливостей для передачі навчання.

Навчання та створення моделі:

- Навчальні моделі: TensorFlow.js підтримує навчання моделей машинного навчання в браузері. Хоча навчання складним моделям глибокого навчання може бути більш обчислювально інтенсивним, воно все ще можливо для завдань меншого масштабу та пропонує чудове середовище для експериментів і навчання.
- Побудова моделі: розробники можуть створювати власні моделі машинного навчання, визначаючи та налаштовуючи рівні, функції

активації та функції втрати за допомогою API високого рівня, наданого TensorFlow.js.

- Управління даними: бібліотека пропонує інструменти для керування та попередньої обробки даних, критично важливі для навчання та оцінки моделі.

Кросплатформна сумісність:

- Інтернет і мобільні пристрої: TensorFlow.js не обмежується веб-браузерами. Його також можна використовувати в мобільних додатках через такі бібліотеки, як TensorFlow Lite для мобільних пристроїв.
- Node.js: TensorFlow.js може працювати в середовищах Node.js, розширюючи його використання за межі браузера до програм на стороні сервера.

Розгортання та оптимізація:

- Оптимізація моделі: TensorFlow.js надає інструменти для оптимізації моделей, включаючи квантування та скорочення, щоб зменшити розмір моделі та покращити швидкість логічного висновку.
- Параметри розгортання: розгортання моделей TensorFlow.js можна здійснювати різними способами, зокрема безпосередньо у веб-додатках, через хмарні служби або в власних мобільних додатках.

Доступність і конфіденційність:

- Доступність: увімкнувши машинне навчання в браузері, TensorFlow.js сприяє тому, щоб зробити ШІ та машинне навчання доступнішими для ширшої аудиторії.
- Конфіденційність. Зберігання даних на стороні клієнта покращує конфіденційність користувачів, зменшуючи потребу надсилати конфіденційну інформацію на зовнішні сервери для обробки.

Майбутні розробки:

- Підтримка WebAssembly: Очікується, що TensorFlow.js виграє від розробки WebAssembly, яка додатково оптимізує виконання моделі та покращить продуктивність.

- Інтеграція з веб-стандартами. Оскільки веб-технології розвиваються, інтеграція з веб-стандартами, такими як WebGPU, може надати розширені можливості апаратного прискорення для TensorFlow.js.

TensorFlow.js — це захоплююча та універсальна технологія, яка дозволяє веб-розробникам інтегрувати машинне навчання у веб-додатки. Його можливості щодо навчання, побудови моделей, крос-платформної сумісності та варіантів розгортання роблять його цінним інструментом для створення рішень на основі штучного інтелекту, які можна запускати безпосередньо в браузері, на мобільних пристроях або в середовищі на стороні сервера. Переваги доступності та конфіденційності бібліотеки відкривають нові можливості для веб-додатків машинного навчання, гарантуючи, що TensorFlow.js і надалі залишатиметься значним гравцем у сфері веб-розробки та машинного навчання, що постійно розвивається.

Далі ми поговоримо про Face-API.js, бібліотеку JavaScript з відкритим вихідним кодом, яка дає розробникам змогу з легкістю виконувати розпізнавання обличчя, розпізнавання орієнтирів обличчя та аналіз виразу обличчя.

Face-API.js — це бібліотека JavaScript, яка набула популярності завдяки своїй здатності виконувати розпізнавання та аналіз обличчя безпосередньо у веб-додатках. Він пропонує потужний набір інструментів і функцій для роботи із зображеннями обличчя, що робить його цінним ресурсом для широкого спектру застосувань, від фільтрів соціальних мереж до систем безпеки та спостереження. У цій статті ми заглибимося в ключові функції та можливості Face-API.js, його програми та етичні міркування, пов’язані з технологією розпізнавання обличчя.
Основні характеристики Face-API.js:
Розпізнавання обличчя:

- Face-API.js відмінно справляється з виявленням обличь у зображеннях і відеопотоках. Він використовує моделі глибокого навчання, щоб ідентифікувати обличчя та їх положення в заданому кадрі.

Орієнтири обличчя:

- Бібліотека може ідентифікувати ключові орієнтири обличчя, такі як очі, ніс і рот, що корисно для таких завдань, як вирівнювання обличчя та аналіз рис.

Розпізнавання обличчя:

- Face-API.js також можна використовувати для розпізнавання облич, дозволяючи розробникам ідентифікувати та зіставляти обличчя на кількох зображеннях або кадрах.

Виявлення емоцій:

- Він може аналізувати вираз обличчя, щоб виявити такі емоції, як щастя, смуток, гнів тощо. Ця функція часто використовується в програмах, пов’язаних з аналізом настроїв і залученням користувачів.

Оцінка віку та статі:

- Бібліотека може оцінити вік і стать людини за рисами обличчя. Це корисно для різноманітних програм, у тому числі для цільового маркетингу та профілювання користувачів.

Фільтри соціальних мереж:

- Багато популярних платформ соціальних медіа використовують Face-API.js, щоб запропонувати користувачам веселі та інтерактивні фільтри та ефекти, які можна застосувати до їхніх фотографій і відео.

Безпека та спостереження:

- Бібліотека використовується в системах безпеки та спостереження для виявлення обличь, ідентифікації та моніторингу в реальному часі. Це може допомогти підвищити безпеку, сповіщаючи органи влади про підозрілих осіб.

Роздрібна торгівля та маркетинг:

- Компанії використовують Face-API.js для профілювання клієнтів і цільової реклами. Це може допомогти зрозуміти демографічні показники та вподобання клієнтів.

Доступність:

- Face-API.js можна використовувати для розробки програм, які допомагають людям з обмеженими можливостями. Наприклад, його можна використовувати для керування комп'ютерними інтерфейсами за допомогою міміки.

Етичні міркування:

- Незважаючи на те, що Face-API.js пропонує вражаючі можливості, він також викликає етичні проблеми:

Конфіденційність:

- Збір і аналіз даних про обличчя може порушувати конфіденційність людей. Чітка згода та заходи захисту даних є важливими.

Упередженість:

- Технологія розпізнавання обличчя, зокрема Face-API.js, може виявляти упередження, що призводить до неточностей і потенційної дискримінації, особливо в малопредставлених групах.

Безпека:

- Використання розпізнавання обличчя в системах безпеки може призвести до вразливості та потенційного зловживання зловмисниками.

Регламент:

- Уряди та регуляторні органи активно працюють над створенням інструкцій і правил відповідального використання технології розпізнавання обличь.

Face-API.js — це універсальна та потужна бібліотека JavaScript для розпізнавання та аналізу обличчя. Його широкий спектр застосувань, від фільтрів соціальних мереж до систем безпеки, робить його цінним ресурсом для розробників. Однак етичні проблеми, пов'язані з конфіденційністю, упередженістю та безпекою, слід ретельно враховувати під час впровадження технологій розпізнавання обличчя. Важливо знайти баланс між інноваціями та відповідальним використанням, щоб гарантувати, що ця технологія принесе користь суспільству без шкоди правам особи та безпеці.

WebGazer.js — це бібліотека JavaScript, яка отримала визнання завдяки інноваційному підходу до веб-відстеження очей. Ця технологія пропонує ряд застосувань, від оптимізації взаємодії з користувачем до покращення доступності на веб-сайтах. У цій статті ми розглянемо ключові функції та можливості WebGazer.js, його програми та етичні міркування, пов’язані з відстеженням очей у цифровій сфері.

Відстеження очей у реальному часі:

- WebGazer.js призначений для відстеження рухів очей користувача в реальному часі. Він використовує методи комп’ютерного зору та машинне навчання, щоб оцінити, куди на екрані дивиться користувач.

Кросбраузерність:

- Бібліотека сумісна з основними веб-браузерами, що робить її доступною для широкого спектру веб-додатків.

Калібрування:

- WebGazer.js містить функції калібрування, які дозволяють користувачам калібрувати систему стеження за очима, забезпечуючи більшу точність відстеження точок погляду.

Збір даних Gaze:

- Розробники можуть збирати дані про погляди, які містять інформацію про те, куди користувачі дивляться на веб-сторінці. Ці дані корисні для аналізу поведінки користувачів і оптимізації веб-вмісту.

Застосування WebGazer.js:

Оптимізація взаємодії з користувачем. WebGazer.js можна використовувати для відстеження того, як користувачі взаємодіють із веб-сайтом, допомагаючи дизайнерам і розробникам визначити сфери інтересів і уваги. Цю інформацію можна використовувати для оптимізації макета та вмісту веб-сторінок.

Доступність. Технологія покращує веб-доступність, дозволяючи користувачам переміщатися та взаємодіяти з веб-вмістом, використовуючи

погляд, роблячи веб-сайти більш інклюзивними для людей з обмеженими можливостями.

Дослідження ринку. Компанії можуть використовувати WebGazer.js для дослідження ринку, щоб зрозуміти, як користувачі взаємодіють із їхніми веб-сайтами, оголошеннями чи продуктами. Ці дані можуть бути цінними для вдосконалення маркетингових стратегій.

Ігри. WebGazer.js можна інтегрувати в веб-ігри, щоб запропонувати інноваційний ігровий процес, який реагує на погляд гравця, забезпечуючи новий вимір інтерактивності.

Етичні міркування. WebGazer.js, як і будь-яка технологія відстеження очей, викликає етичні проблеми:

Конфіденційність. Збір даних погляду може порушити конфіденційність користувачів. Важливо отримати інформовану згоду та дотримуватися суворих практик захисту даних.

Безпека. Існує ризик несанкціонованого доступу до даних перегляду, що потенційно може призвести до порушень безпеки. Розробники повинні впровадити надійні заходи безпеки для захисту конфіденційної інформації.

Згода користувача. Веб-сайти, які використовують WebGazer.js, повинні чітко інформувати користувачів про збір даних і гарантувати, що вони погоджуються на відстеження їхнього погляду.

Обробка даних. Розробники повинні відповідально ставитися до зібраних даних погляду, знеособлюючи їх, коли це можливо, і дотримуючись правових і етичних інструкцій щодо зберігання та використання даних.

WebGazer.js — це піонерська технологія, яка пропонує можливості відстеження очей у режимі реального часу в Інтернеті, забезпечуючи низку програм від оптимізації взаємодії з користувачем до покращення доступності. Однак відповідальне використання цієї технології має вирішальне значення для вирішення питань конфіденційності та безпеки. Встановлення балансу між інноваціями та етичними міркуваннями має важливе значення для того, щоб

WebGazer.js приносив користь користувачам і суспільству в цілому, одночасно захищаючи індивідуальні права та конфіденційність.

Як працює WebGazer.js? WebGazer.js використовує методи комп'ютерного зору та алгоритми машинного навчання, щоб оцінити точку погляду користувача на веб-сторінці. Він працює шляхом аналізу каналу веб-камери користувача, відстеження рухів його очей і відображення цих рухів у координатах на екрані.

Процес калібрування. Щоб забезпечити точне відстеження погляду, WebGazer.js зазвичай вимагає процесу калібрування. Під час калібрування користувачам пропонується стежити за своїм поглядом на певні точки або об'єкти на екрані. Потім система використовує цю інформацію для створення функції відображення для точної оцінки погляду.

Кросбраузерність. WebGazer.js розроблений для роботи з основними веб-браузерами, включаючи Google Chrome, Mozilla Firefox та іншими, що робить його доступним для широкого кола користувачів. Ця сумісність дозволяє веб-розробникам легко інтегрувати функцію відстеження очей у свої веб-програми.

Збір та аналіз даних. WebGazer.js може збирати та надавати дані про те, де користувачі переглядають веб-сторінку, які можна аналізувати для різних цілей. Ці дані зазвичай мають форму координат x-y, що вказують точки погляду. Веб-розробники можуть використовувати цю інформацію, щоб отримати уявлення про поведінку користувачів, теплові карти або запустити певні дії на основі взаємодії погляду.

Застосування. Оптимізація взаємодії з користувачем: WebGazer.js використовується для розуміння того, як користувачі взаємодіють із веб-сайтом або веб-додатком, допомагаючи дизайнерам і розробникам удосконалити роботу з користувачем.

Доступність. Це робить веб-сайти більш доступними, дозволяючи користувачам переміщатися, прокручувати та взаємодіяти з веб-вмістом за допомогою погляду. Це корисно для людей з обмеженими можливостями, які можуть мати труднощі з використанням традиційних методів введення.

Дослідження ринку. Компанії можуть використовувати технологію для дослідження ринку, відстежуючи взаємодію користувачів із їхніми продуктами, рекламою та веб-вмістом.

Етичні міркування. Як і у випадку з будь-якою іншою технологією, яка передбачає збір даних, під час впровадження WebGazer.js важливі міркування щодо конфіденційності та етики. Дані Gaze можуть бути конфіденційними, тому користувачі повинні бути проінформовані та надати згоду на відстеження. Для захисту зібраних даних мають бути вжиті заходи безпеки, а розробники мають дотримуватися найкращих практик щодо обробки та зберігання даних.

З відкритим кодом і на основі досліджень. WebGazer.js є проектом з відкритим кодом, що означає, що код і результати дослідження доступні для громадськості. Така відкритість заохочує співпрацю та дозволяє розробникам налаштовувати та розширювати бібліотеку відповідно до своїх конкретних потреб.

У програмному модулі використовується поняття евклідової відстані, також відомої як евклідова метрика. Ця метрика визначає звичайну відстань між 2-ма точками у просторі, таку, яку можна виміряти, якщо використовувати лінійку. На рисунку 3.1 наведено два приклади обчислення 3-ох евклідових дистанцій між відповідними точками обличчя.

Перша евклідова відстань, позначена як «d1,» вимірює дистанцію між верхньою частиною носа та зовнішнім кутом правого ока. Друга евклідова відстань, позначена як «d2,» визначає дистанцію між верхньою частиною носа та внутрішнім кутом лівого ока. Нарешті, третя евклідова відстань, позначена як «d3,» вказує на дистанцію між вершиною носа та лівим кутом рота.

Ці відстані між відповідними точками обличчя важливі для багатьох задач, пов’язаних із обробкою зображень та розпізнаванням обличчя. Вони можуть бути використані для аналізу форми обличчя, визначення виразів обличчя та інших досліджень, які базуються на розташуванні точок на обличчі.

Евклідова відстань є важливим інструментом у великій кількості областей, включаючи комп’ютерне бачення, обробку зображень, глибоке навчання та

багато інших застосувань. Вона допомагає кількісно оцінити відстані між точками, що може бути використаною для подальшого аналізу та прийняття рішень в різних завданнях.

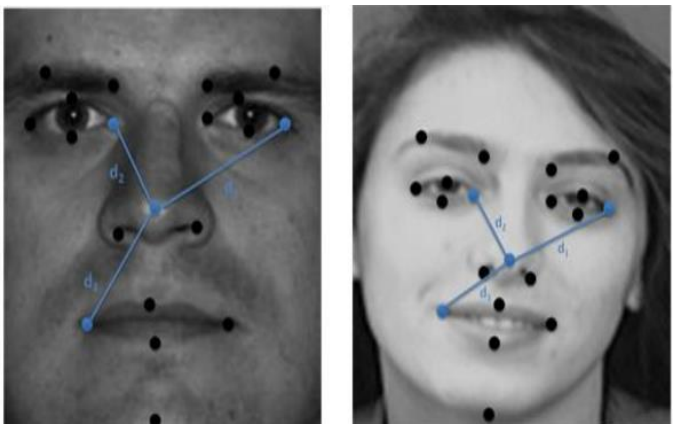


Рис. 3.1 Приклади 3-х евклідових дистанцій між характерними точками.

$$d(P,Q) = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2} \tag{3.1}$$

$$d(P,Q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + (p_3 - q_3)^2} \tag{3.2}$$

Зазначені формули (3.1) і (3.2) визначають спосіб розрахунку евклідової відстані між точками у евклідовому просторі, де n визначає розмірність простору (наприклад, n = 2 для двовимірного простору і n = 3 для тривимірного простору). Ці формули базуються на понятті відстані між двома точками P і Q, де P представлено координатами (p_1, p_2, …, p_n), і Q представлено координатами (q_1, q_2, …, q_n).

У формулі (3.1), відстань між P і Q обчислюється, як корінь квадратний з суми квадратів різниць відповідних координат p_i і q_i. Це загальний вираз для обчислення евклідової відстані в n-просторі.

У формулі (3.2), специфічно для тривимірного простору, відстань обчислюється, як корінь квадратний з суми квадратів різниць координат p_1 і q_1, p_2 і q_2, p_3 і q_3. Ця формула застосовується, коли точки P і Q представлені тривимірними координатами.

Евклідова відстань часто використовується у багатьох областях, включаючи морфометрію та розпізнавання обличчя. У контексті розпізнавання обличчя, якщо унікальні точки обличчя були отримані з зображень, відстані між цими мітками можуть служити для порівняння різних обличь. Це допомагає

визначити ступінь схожості між обличчями, що є важливим у завданнях систем розпізнавання та аутентифікації.

3.2. Архітектура програмного модуля

Переходимо до нашого програмного модулю. Він буде складатися з двох вебпрограм (веб-сайтів). Перша програма буде відповідати за аналіз та перевірку особистості. Друга вебпрограма буде продовженням першої. Вона буде проводити ідентифікацію за напрямком погляду користувача. Місце, куди потрібно дивитися користувач повинен вибирати ще на першій стадії ідентифікації (на першому веб-сайті).

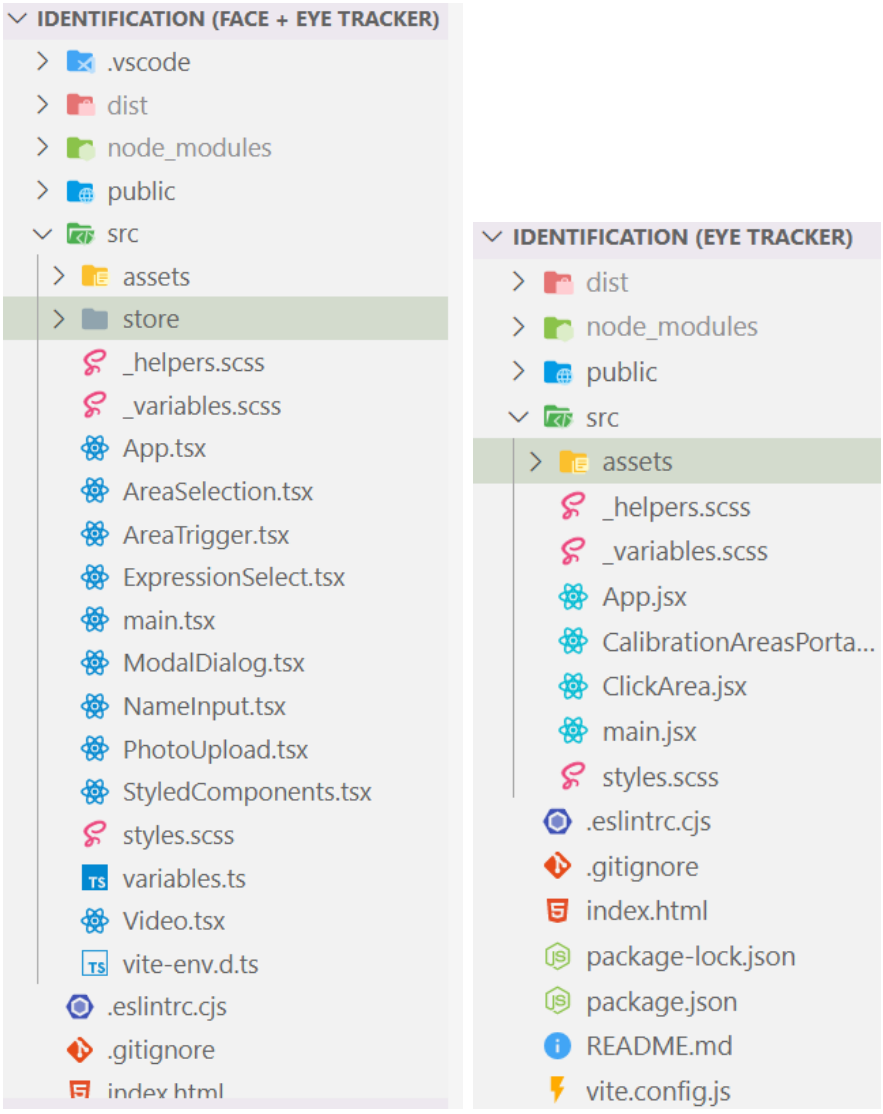


Рис. 3.2 Архітектура двох програмних модулів (ліворуч – модуль розпізнавання по обличчю, праворуч – модуль відстеження очей)

Наше програмне забезпечення буде працювати на основі бібліотеки React, яка складається з компонентів. Ці компоненти відіграють свої ключові ролі. Опишемо папки та ролі файлів у цих папках:

- Папка «.vscode» - папка, яка створюється за рахунок роботи у програмі VS Code. Там містяться файли, які відповідають лише за роботу та налаштування програми VS Code.
- Папка «dist» - це папка, яка містить збілдований проект нашої програми. Вона відіграє роль готового проекту, який в кінці розробки є збілдованим та готовим.
- Папка «node_modules» - це папка, яка містить бібліотеки, фреймворки та інші програмні забезпечення для роботи нашого програмного модулю. Саме там розташовані наші бібліотеки по розпізнаванню обличчя та детектора руху очей.
- Папка «public» - це папка, де розташовані заготовлені та навчені моделі, які допомагають розпізнаванню обличчя (див. рис. 3.3).

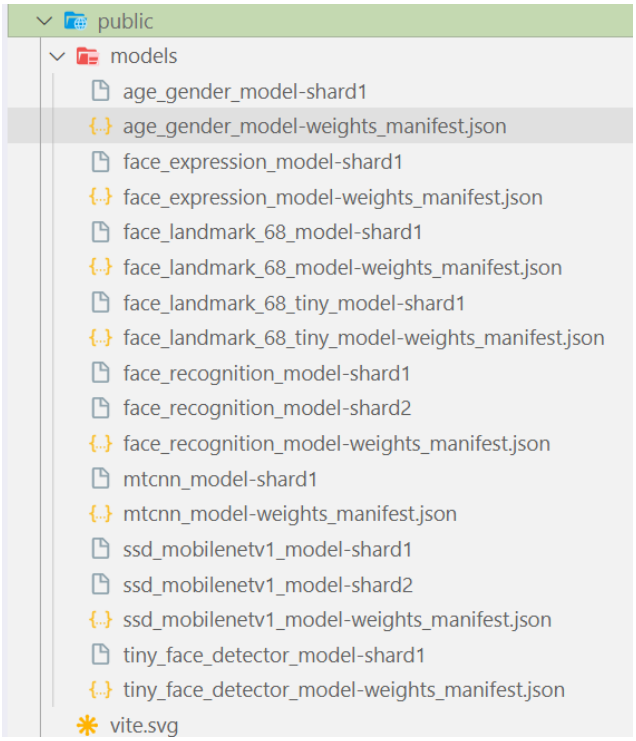


Рис. 3.3 Моделі у папці, які є одним з ключових етапів роботи програмного модулю.

- Далі йде папка «src» - це коренева папка, де розташований наш програмний модуль. В ній розташовані робочі файли нашого програмного модулю. В ній є декілька папок та файлів:
    - Папка «assets» - там містяться вторинні файли, які відповідають за декоративні частини нашого програмного модуля, а саме картинки, тощо.
    - Папка «store» - це папка, яка є ключовим фактором у Redux. Саме там будуть зберігатися фото користувача, його ім’я, вибір емоції, місце погляду.
    - Декілька файлів з розширенням «.scss». Ці файли використовуються лише для стилізації програмного модулю.
    - «AreaSelection.tsx», «AreaTrigger.tsx», «ExpressionSelect.tsx», «ModalDialog.tsx», «NameInput.tsx», «PhotoUpload.tsx», «Video.tsx» - компоненти додатку. Компоненти відповідають за відображення окремих частин інтерфейсу користувача програми.
    - Файл «vite.config.ts» містить конфігурацію програми Vite. У цьому файлі можна настроїти такі параметри, як маршрутизація, статичні ресурси тощо.
    - Файл «tsconfig.json» містить конфігурацію компілятора TypeScript. У цьому файлі можна налаштувати такі параметри, як версії TypeScript, що підтримуються, типи файлів і т.д.
    - Файл «package.json» містить метадані про програму. У цьому файлі можна вказати такі відомості, як назва програми, версія, залежності тощо.

Так само у наступній програмі. Там є схожі файли та компоненти, але вже вони відповідають за детектор руху очей та подальшу ідентифікацію.

3.3. Експлуатація програмного модулю

Для експлуатації даного програмного модуля буде використовуватися веб середовище. Користувачу необхідно буде перейти на вебсторінку за URL адресою (https://github.com/JohnnieWalked/faceID-eyeTracker-react) та почати подальший процес ідентифікації. Його буде зустрічати наступний графічний інтерфейс (див. рис. 3.4).

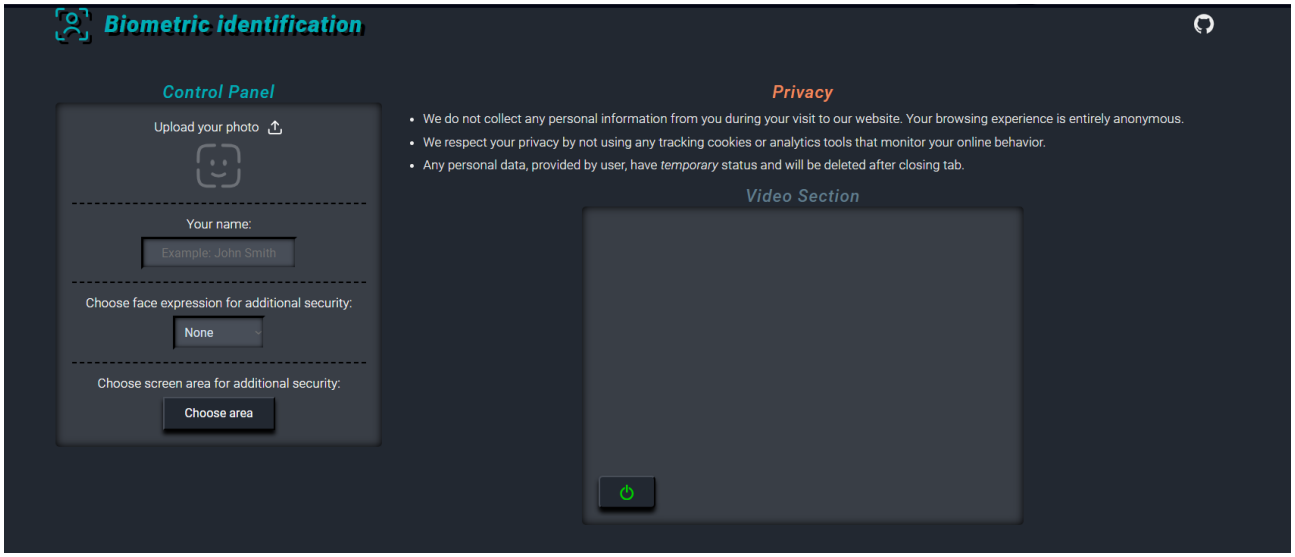


Рис. 3.4 Графічний інтерфейс програмного засобу

На самому початку після входу на вебсторінку буде завантаження моделей бібліотеки face-api.js. Це необхідно для аналізу фотографії, яку користувач буде завантажувати на вебсторінку.

Найголовнішою секцію даного програмного модулю є Контрольна Панель (див. рис. 3.5). Саме там користувач завантажує своє фото, вводить у відповідне поле своє ім’я чи псевдонім, який буде використовуватися для створення мітки. Також присутній вибір емоції, яку користувач повинен зобразити на своєму обличчі для подальшого проходження ідентифікації. Також наявна функція вибору області екрану, де повинен зосереджуватися погляд користувача під час проходження ідентифікації.

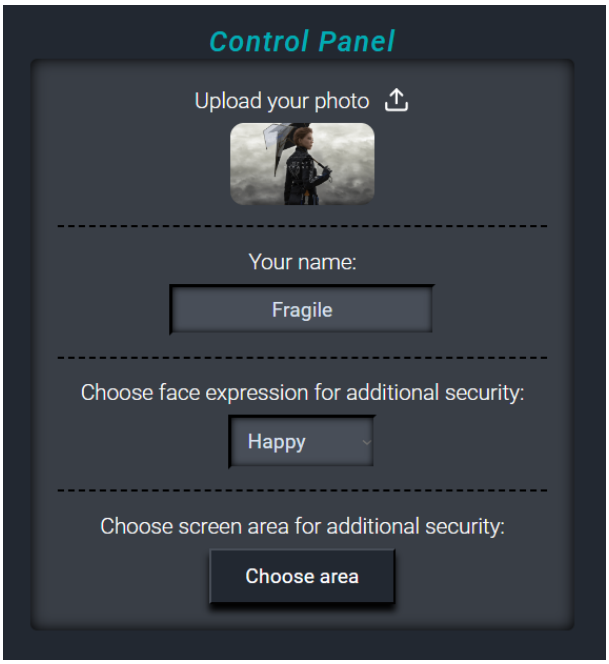


Рис. 3.5 Заповнена «Контрольна Панель»

Після заповнення панелі, наступним кроком є запуск вебкамери. Після натискання кнопки «Пуску», запускається камера та починається процес ідентифікації. Якщо буде якась помилка, програма даси користувачу про це знати.

Для прикладу ми завантажили зображення однієї героїні з гри автора Хідео Кодзіми, а саме гри «Death Stranding». Тепер перевіримо, як буде працювати програма, коли буде показано не те обличчя, яке очікує програма (див. рис. 3.6).

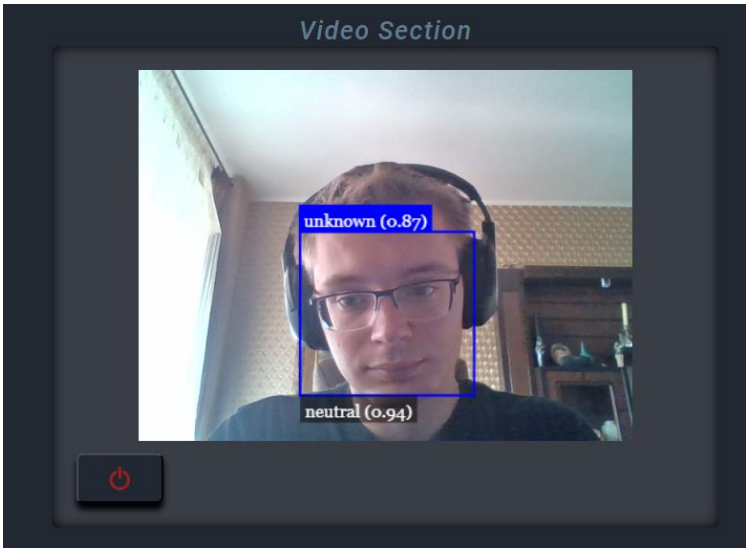


Рис. 3.6 Тестовий приклад не збігання аналізу.

Тепер перевіримо як буде працювати після збігу аналізу відео.

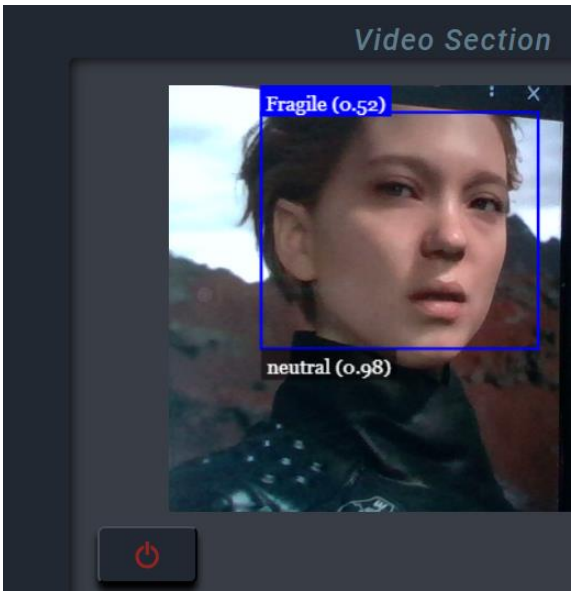


Рис. 3.6 Тестовий приклад збігання аналізу.

Але емоція не збігається, ось тут ми бачимо вже перші переваги досконалого програмного модулю біометричної ідентифікації. Навіть якщо перехитрити програму та показати фотографію, емоція буде не збігатися, чи погляд у відповідну область теж буде не збігатися. Тепер перевіримо на живому прикладі.

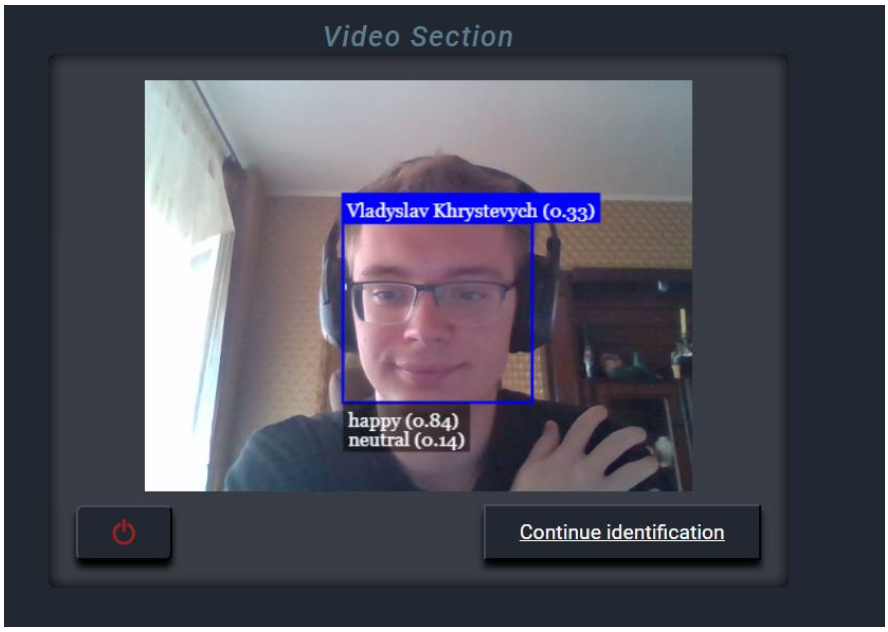


Рис. 3.7 Тестовий приклад успішного проходження першої фази ідентифікації.

Після натискання кнопки «Continue identification» нас перекидає на другу фазу проходження ідентифікації.

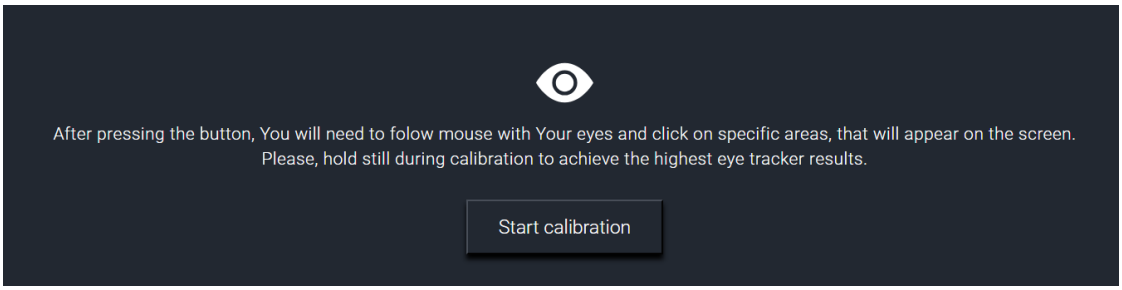


Рис. 3.8 Друга фаза проходження ідентифікації.

На цьому етапі вже треба дотримуватися інструкцій програми. Як ми бачимо, користувача просять дотримуватися відповідних умов. Користувачу необхідно пройти перевірку куди саме він кидає свій погляд. Для цього програма запускає бібліотеку машинного навчання комп'ютерного зору (webgazer.js). Користувачу буде необхідно дивитися у відповідні ділянки екрану та клацати мишкою по цим ділянкам. Також дуже важливо тримати свій погляд у тій зоні, куди ви клацаєте.

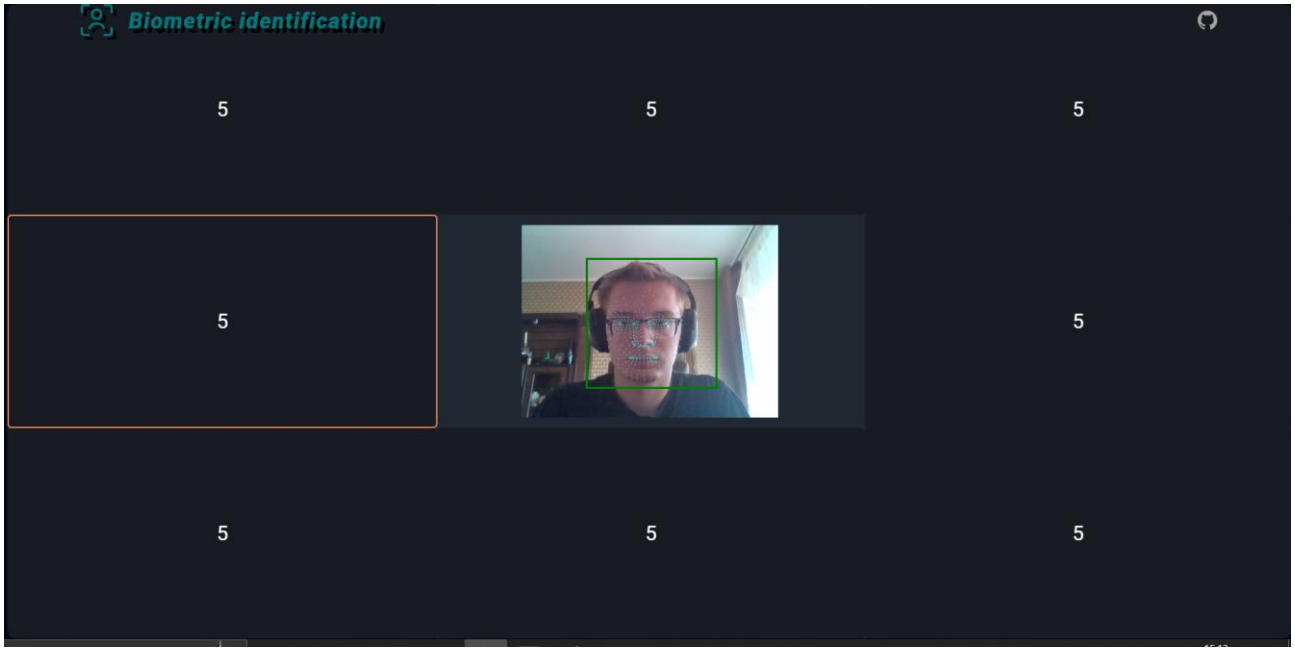


Рис. 3.9 Процес аналізу та машинного навчання.

Як ми бачимо, користувачу необхідно клацати мишею по відповідним ділянкам. Після цього, починається вже процес ідентифікації. На екрані з'явиться червона крапка, яка буде показувати куди саме дивиться користувач. Хочу це не дуже точний показ, це краще називати передбаченням, оскільки програма не гарантує 100% точний аналіз погляду.

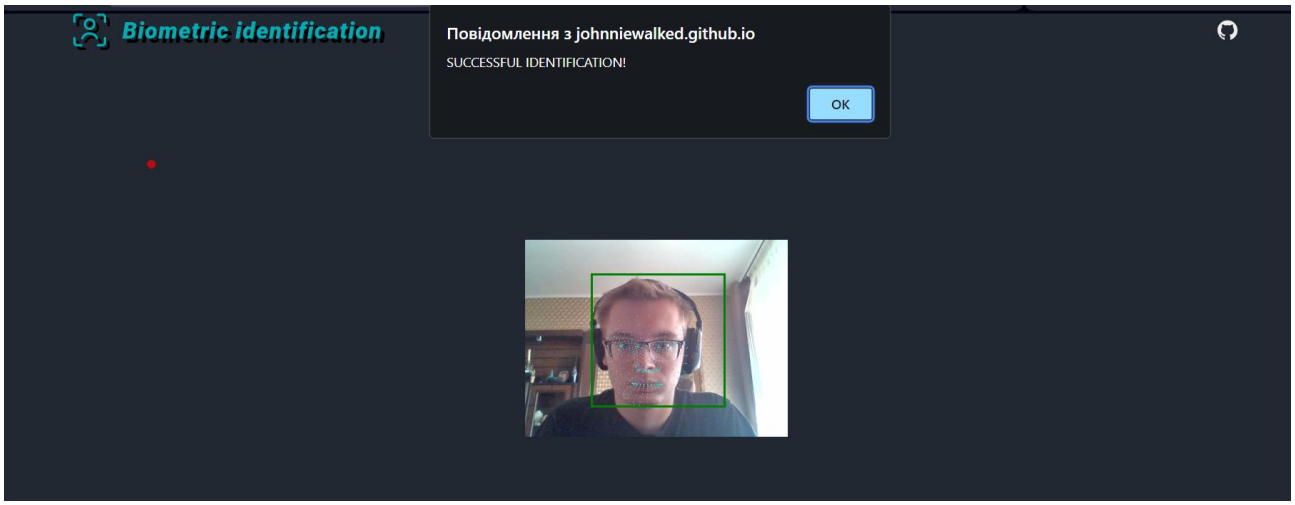


Рис. 3.10 Успішне проходження ідентифікації.

3.4. Висновки до третього розділу.

Недоліком існуючої системи ідентифікації користувача за обличчям є використання декартової системи координат, що створює можливість обхіду системи за допомогою фотографії користувача. Проте відзначається, що визначення залежить від вигляду обличчя, яке знаходиться у базі даних, і може обмежуватися певними емоціями, такими як посмішка чи похмурість.

Аналізуючи бібліотеку face-api.js, виявлено, що носіння окулярів може суттєво вплинути на результати детектування обличчя, що може бути важливим для використання в різних областях, зокрема в Україні, де біометричні дані отримують без окулярів і в тривимірному просторі.

Технологічні рішення для ідентифікації обличчя різняться, проте TensorFlow виокремлюється як потужна бібліотека, що служить основою для інших, таких як face-api.js.

Безпека бази даних підкреслюється обмеженим доступом лише для адміністратора сервера, що додає шар захисту від несанкціонованого доступу та внесення даних. У той же час, наголошується на потребі потужного обладнання для ефективної обробки моделей у базі даних, що визначає важливість використання потужних процесорів та багатоядерних систем.

Комбінування різних методів ідентифікації, таких як face ID, відбиток пальця, система відстеження погляду користувача та двофакторна автентифікація, визначається як підвищений рівень захисту особистих даних від несанкціонованого доступу. Бібліотека webgazer.js допомагає підвищити рівень безпеки проходження ідентифікації.

РОЗДІЛ 4. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

4.1 Екологічне законодавство

Екологічне законодавство України – це ціла система нормативно-правових актів, що містять еколого-правові норми, які здатні регулювати екологічні правовідносини, що виникають у галузі використання природних ресурсів, охорони навколишнього природного середовища і забезпечення екологічної безпеки.

Система екологічного законодавства України є досить прогресивною, тому що вона створювалася вже в умовах незалежності з використанням досвіду світових лідерів, в галузі екологічного права. Сьогодні ми можемо сміливо констатувати, що той "правовий вакуум" в сфері охорони довкілля і екологічної безпеки, що утворився одразу після проголошення незалежності ліквідовано. За ці роки в Україні прийнято кілька десятків законів та кодексів що регулюють всю гамму екоправових відносин у державі.

Міжнародне екологічне право. Розв'язання сучасних екологічних проблем в Україні можливе тільки в умовах широкого й активного міжнародного співробітництва всіх країн у цій сфері. Це зумовлено насамперед такими обставинами:

- глобальним характером екологічних проблем;
- транскордонним характером забруднення навколишнього середовища;
- міжнародними зобов'язаннями України щодо охорони навколишнього природного середовища;
- необхідністю міжнародного обміну досвідом і технологіями, можливістю залучення іноземних інвестицій.

Україна є учасником понад 20 міжнародних конвенцій та двосторонніх угод, пов'язаних з охороною навколишнього природного середовища. Міжнародні зобов'язання України щодо навколишнього природного середовища, використання природних ресурсів і забезпечення екологічної

безпеки випливають з положень вже ратифікованих а також тих, що знаходяться в стадії розгляду конвенцій та угод. Виконання Україною зобов'язань, що випливають із зазначених багатосторонніх угод, потребує приведення внутрішнього законодавства у відповідність з нормами міжнародного права й урахування існуючої міжнародної практики під час розроблення нових законодавчих актів.

Основу екологічного законодавства України складають Конституція України, закони України «Про охорону навколишнього природного середовища», «Про охорону атмосферного повітря», «Про охорону земель», «Про охорону вод», «Про охорону тваринного світу», «Про охорону рослинного світу», «Про охорону біосфери», «Про охорону атмосферного повітря в місті Києві» та інші.

Ці закони визначають основні принципи та напрями охорони навколишнього природного середовища, встановлюють права та обов'язки суб'єктів екологічних правовідносин, встановлюють систему органів виконавчої влади та місцевого самоврядування, які здійснюють охорону навколишнього природного середовища.

Крім законів, до екологічного законодавства України також належать:

- підзаконні нормативно-правові акти, які видаються Кабінетом Міністрів України, центральними органами виконавчої влади, органами виконавчої влади Автономної Республіки Крим, обласними, Київською та Севастопольською міськими, районними, районними у містах, районними у місті Києві державними адміністраціями;
- міжнародні договори України, які стосуються охорони навколишнього природного середовища;
- нормативно-правові акти органів місцевого самоврядування, що стосуються охорони навколишнього природного середовища.

Екологічне законодавство України спрямоване на:

- забезпечення екологічної безпеки населення;
- збереження біологічного і ландшафтного різноманіття;

- раціонального використання природних ресурсів;
- відновлення природних ресурсів, що зазнали виснаження.

Екологічне законодавство України є важливою складовою правової системи України. Воно забезпечує захист навколишнього природного середовища, яке є основою існування і розвитку людського суспільства.

Основні принципи екологічного законодавства України:

- пріоритет охорони навколишнього природного середовища перед економічним розвитком;
- комплексний підхід до охорони навколишнього природного середовища;
- запобігання негативному впливу на навколишнє природне середовище;
- відповідальність за порушення екологічного законодавства.

Права та обов'язки суб'єктів екологічних правовідносин. Суб'єкти екологічних правовідносин – це фізичні та юридичні особи, які беруть участь у відносинах, пов'язаних з охороною навколишнього природного середовища.

Права суб'єктів екологічних правовідносин включають:

- право на безпечне для життя і здоров'я навколишнє природне середовище;
- право на участь у охороні навколишнього природного середовища;
- право на відшкодування збитків, завданих порушенням екологічного законодавства.

Обов'язки суб'єктів екологічних правовідносин включають:

- обов'язок дотримуватися вимог екологічного законодавства;
- обов'язок не допускати негативного впливу на навколишнє природне середовище;
- обов'язок вживати заходів щодо відшкодування збитків, завданих порушенням екологічного законодавства.

Система органів виконавчої влади та місцевого самоврядування, які здійснюють охорону навколишнього природного середовища:

- Верховна Рада України;
- Кабінет Міністрів України;
- центральні органи виконавчої влади;

- органи виконавчої влади Автономної Республіки Крим;
- обласні, Київська та Севастопольська міські, районні, районні у містах, районні у місті Києві державні адміністрації;
- органи місцевого самоврядування.

Відповідальність за порушення екологічного законодавства:

- дисциплінарна;
- адміністративна;
- цивільна;
- кримінальна.

Екологічне законодавство України постійно вдосконалюється. Ухвалюються нові закони та підзаконні нормативно-правові акти, спрямовані на посилення охорони навколишнього природного середовища.

ВИСНОВКИ

Результати виконаної кваліфікаційної роботи включають в себе розробку програмного модулю для біометричної ідентифікації, який базується на аналізі обличчя за допомогою камери у режимі реального часу та наступній перевірці ділянки погляду користувача. У процесі виконання роботи отримані такі результати:

- проведений аналіз різних методів біометричної ідентифікації дозволяє визначити їхні особливості та визначити найбільш поширені та ефективні з точки зору витрат методи;
- виконаний аналіз проблем і вразливостей методів біометричної ідентифікації визначає можливі ризики, які може зіткнутися користувач, що є важливою інформацією для подальшого вдосконалення системи.;
- вивчені та проаналізовані механізми реалізації біометричних технологій, зокрема застосування нейронних мереж та вебтехнологій, що визначає можливості реалізації біометричної ідентифікації;
- описано взаємодію машинного навчання та комп’ютерного зору, їхні види та різновиди механізмів реалізації, що вказує на актуальність та використання цих технологій у сучасному світі;
- описано та реалізовано функціональні характеристики програмного модулю розпізнавання обличь та середовище його функціонування, що призводить до створення програмного модулю, придатного для використання у веб-середовищах;
- надано результати тестових прикладів роботи програмного модулю, що підтверджують його ефективність та можливість експлуатації в інших системах для зменшення ризику несанкціонованого доступу та підвищення рівня безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Закон України «Про положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/1073-2017-п#Text
2) Закон України «Про захист персональних даних» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/2297-17#Text
3) Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/5492-17#Text
4) Закон України «Про захист інформації в інформаційно-комунікаційних системах» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
5) Закон України «Про інформацію» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/2657-12#Text
6) Закон України «Про електронні документи та електронний документообіг» [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/851-15#Text
7) Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks (Advances in Computer Vision and Pattern Recognition) 1st ed. 2022 Edition / Christian Rathgeb, Ruben Tolosana, Ruben Vera-Rodriguez, Christoph Busch (англ.) – P. 27-43
8) What is biometric authentication? (англ.) [Електронний ресурс]. Режим доступу - https://www.techtarget.com/searchsecurity/definition/biometric-authentication
9) One Millisecond Face Alignment with an Ensemble of Regression Trees (англ.) [Електронний ресурс]. Режим доступу - https://www.csc.kth.se/~vahidk/papers/KazemiCVPR14.pdf

10) FaceNet: A Unified Embedding for Face Recognition and Clustering (англ.) [Електронний ресурс]. Режим доступу - https://www.cv-foundation.org/openaccess/content_cvpr_2015/app/1A_089.pdf

11) MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications (англ.) [Електронний ресурс]. Режим доступу - https://arxiv.org/pdf/1704.04861.pdf

12) Програмна бібліотека TensorFlow [Електронний ресурс]. Режим доступу - https://www.tensorflow.org

13) Програмна бібліотека face-api.js (англ.) [Електронний ресурс]. Режим доступу - https://justadudewhohacks.github.io/face-api.js/docs/index.html

14) Euclidean & Geodesic Distance between a Facial Feature Points in Two-Dimensional Face Recognition System (англ.) [Електронний ресурс]. Режим доступу - https://www.researchgate.net/publication/311924096_Euclidean_Geodesic_Distance_between_a_Facial_Feature_Points_in_Two-Dimensional_Face_Recognition_System#:~:text=The%20Euclidean%20distance%20between%20landmarks,compute%20the%20corresponding%20Euclidean%20distances

15) MobileNets: Open-Source Models for Efficient On-Device Vision (англ.) [Електронний ресурс]. Режим доступу - https://ai.googleblog.com/2017/06/mobilenets-open-source-models-for.html

16) MobileNetV2: The Next Generation of On-Device Computer Vision Networks (англ.) [Електронний ресурс]. Режим доступу - https://ai.googleblog.com/2018/04/mobilenetv2-next-generation-of-on.html

17) Convolutional Neural Networks (англ.) [Електронний ресурс]. Режим доступу - https://www.coursera.org/learn/convolutional-neural-networks

18) MobileNet (англ.) [Електронний ресурс]. Режим доступу - https://www.coursera.org/lecture/convolutional-neural-networks/mobilenet-B1kPZ

19) Modern Face Recognition with Deep Learning (англ.) [Електронний ресурс]. Режим доступу - https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78

20) SSD: Single Shot MultiBox Detector (англ.) [Електронний ресурс]. Режим доступу - https://arxiv.org/abs/1512.02325

21) SSD: Single Shot MultiBox Detector (англ.) [Електронний ресурс]. Режим доступу - https://link.springer.com/chapter/10.1007/978-3-319-46448-0_2

22) SSD object detection: Single Shot MultiBox Detector for real-time processing (англ.) [Електронний ресурс]. Режим доступу - https://jonathan-hui.medium.com/ssd-object-detection-single-shot-multibox-detector-for-real-time-processing-9bd8deac0e06

23) SSD: Single Shot MultiBox Detector (англ.) [Електронний ресурс]. Режим доступу - https://link.springer.com/chapter/10.1007/978-3-319-46448-0_2

24) Histograms of Oriented Gradients for Human Detection (англ.) [Електронний ресурс]. Режим доступу - https://lear.inrialpes.fr/people/triggs/pubs/Dalal-cvpr05.pdf

25) Computer Vision vs. Machine Learning: What are the Differences? (англ.) [Електронний ресурс]. Режим доступу - https://kili-technology.com/data-labeling/computer-vision/computer-vision-and-machine-learning-differences

26) face-api.js : A way to build a Face Recognition system in the browser. (англ.) [Електронний ресурс]. Режим доступу - https://medium.com/theleanprogrammer/face-api-js-a-way-to-build-face-recognition-system-in-browser-c1f4ac922657

27) Face Recognition with FaceNet and MTCNN (англ.) [Електронний ресурс]. Режим доступу - https://arsfutura.com/magazine/face-recognition-with-facenet-and-mtcnn/

28) Facial recognition system (англ.) [Електронний ресурс]. Режим доступу - https://en.wikipedia.org/wiki/Facial_recognition_system

29) Face API (англ.) [Електронний ресурс]. Режим доступу - https://azure.microsoft.com/en-us/services/cognitive-services/face/#overview

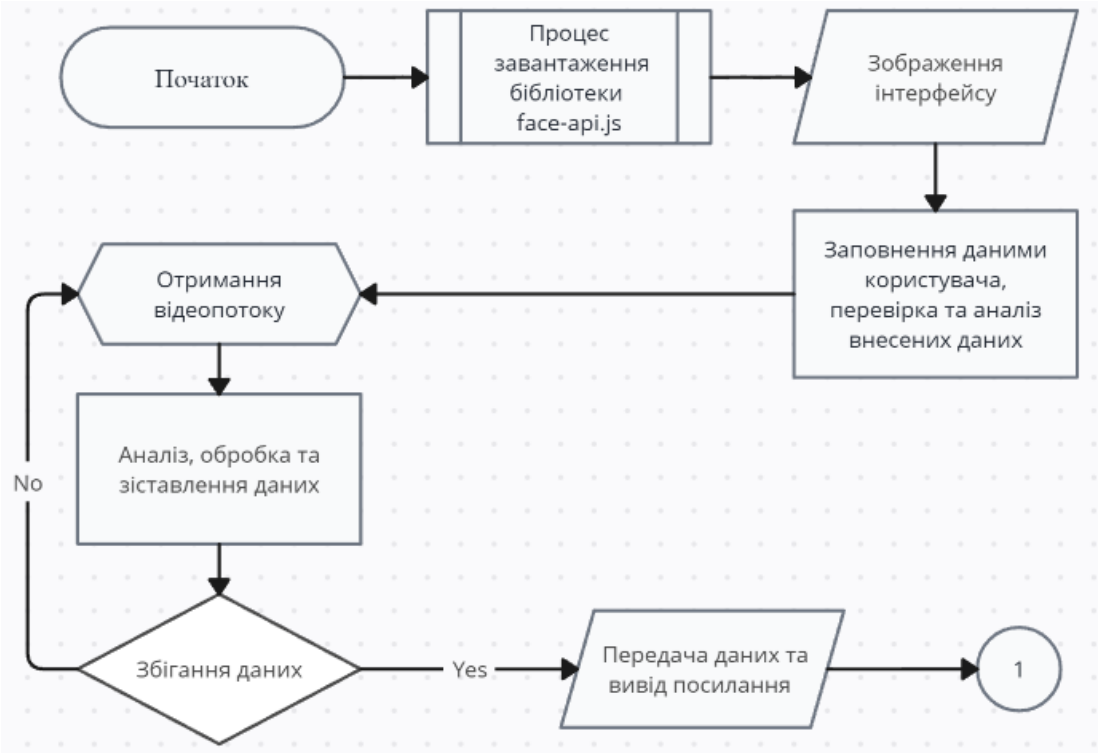
30) Face Identification (англ.) [Електронний ресурс]. Режим доступу - https://www.sciencedirect.com/topics/computer-science/face-identification

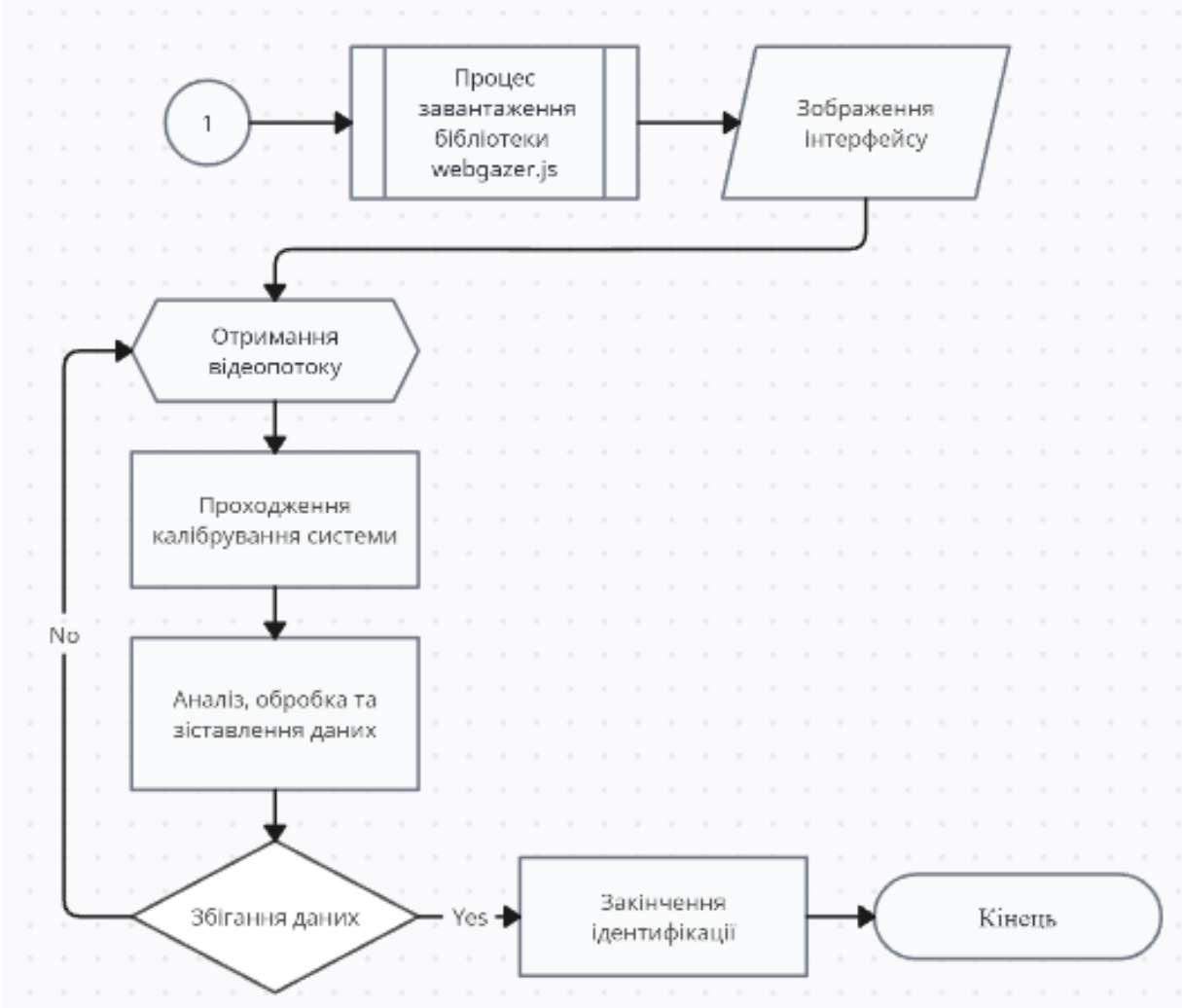
31) Face IDentification (англ.) [Електронний ресурс]. Режим доступу - https://faceidentification.pro

32) Computer Vision vs. Machine Learning | How Do They Relate? (англ.) [Електронний ресурс]. Режим доступу - https://www.weka.io/learn/ai-ml/computer-vision-vs-machine-learning/

33) Machine learning and face recognition (англ.) [Електронний ресурс]. Режим доступу - https://www.pxl-vision.com/en/blog/machine-learning-and-how-it-applies-to-facial-recognition-technology

ДОДАТОК А





Блок-схема функціонування програмного модулю