КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет інформаційних технологій

Кафедра технологій управління

Спеціальність 122 - Комп'ютерні науки
Освітня програма "Інформаційна аналітика та впливи"

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему:

«Дослідження залежності зовнішності злочинців від виду скоєного ним злочину методами машинного навчання»

Студента 2-го курсу групи ІАВ-21

Мудрої Анастасії Денисівни
(прізвище, ім'я, по батькові)

(підпис студента)

Науковий керівник:

кандидат технічних наук, доцент
(науковий ступінь, вчене звання)

Єгорченков Олексій Володимирович
(прізвище, ім'я, по батькові)

(дата) *(підпис)*

Попередній захист:

(Висновок: "До захисту в Державній екзаменаційній комісії")

Завідувач кафедри
технологій управління

(підпис) *(прізвище, ініціали)* *(дата)*

Київ – 2022

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет інформаційних технологій

Кафедра технологій управління
Освітньо-кваліфікаційний рівень Магістр
Спеціальність 122 - Комп'ютерні науки
Програма Інформаційна аналітика та впливи

ЗАТВЕРДЖУЮ
Завідувач кафедри
професор Морозов В.В.

_____
"____" _____20___року

З А В Д А Н Н Я
НА ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Студент Мудра Анастасія Денисівна

Група ІАВ-21

1. Тема кваліфікаційної роботи
Дослідження певних особливостей, скоєного людиною правопорушення, через зовнішні характеристики

Затверджена наказом по від "___"_____20__ р. № ___.

2. Строк подання студентом готової роботи - "___"_____ 20___ р.

3. Цільова установка та вихідні дані до роботи: Дослідити ступінь залежності зовнішності злочинця та видом його злочину
_____
_____
_____

4. Зміст роботи: визначити та описати предметну область дослідження, проаналізувати існуючі рішення, дослідити доступні бази даних для дослідження, проаналізувати методи для вирішення поставленої задачі, проаналізувати засоби для вирішення поставленої задачі, визначити вхідні данні для дослідження, розробити модель для дослідження, візуалізувати отримані результати, розробити інтерфейс програми прогнозування._____
_____
_____

5. Перелік графічного матеріалу (слайдів)
27 рисунків, 1 формула, 4 додатків, 15 слайдів презентації.
_____
_____
_____

6. Календарний план виконання роботи:

№ п/п	Назва частин роботи	%	Виконання роботи	
			За планом	Фактично
1.	Вивчення літературних джерел з предмету дослідження	15	01.10.21	01.10.21
2.	Збір і вивчення матеріалів досліджуваного підприємства	5	24.12.21	24.12.21
3.	Складання розгорнутого плану кваліфікаційної роботи	5	07.01.22	07.01.22
4.	Ознайомлення наукового керівника з розгорнутим планом кваліфікаційної роботи. Внесення змін.	10	18.01.22	18.01.22
5.	Підготовка розділу 1 „Постановка задачі та аналіз рішення”	15	19.01.22 - 20.01.22	19.01.22 - 20.01.22
6.	Підготовка розділу 2 «Концептуалізація інформаційного забезпечення дослідження методами машинного навчання»	20	14.02.22	14.02.22
7.	Підготовка розділу 3 «Побудова моделі прогнозування скоєного злочину по зовнішності з використанням інформаційного забезпечення»	15	08.03.22	08.03.22
8.	Підготовка розділу 4 «Розробка інформаційного забезпечення прогнозування скоєного злочину по зовнішності та рекомендації щодо його використання»	10	01.04.22	01.04.22
9.	Оформлення кваліфікаційної роботи	5	03.05.22	03.05.22
10.	Передача кваліфікаційної роботи рецензенту для рецензування		04.05.22	04.05.22
11.	Передача кваліфікаційної роботи науковому керівникові		11.05.22	11.05.22
12.	Попередній захист		17.05.22	17.05.22

	кваліфікаційної роботи			

Дата видачі завдання “____” _____ 20__ р.

Керівник роботи _____
(посада, прізвище, ім’я, по батькові)

_____
(підпис)

Завдання прийняв до виконання студент групи ІАВ-21

Мудра Анастасія Денисівна
(прізвище, ім’я, по батькові)

_____
(підпис)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SNN - standard neural network – стандартна нейронна мережа;

CNN - convolutional neural network - згорткова нейронна мережа;

ЗНМ – згорткова нейронна мережа;

НМ – нейронна мережа;

KNN - k nearest neighbors – k найближчих сусідів;

SVM - support vector machines – опорний вектор;

ReLu - rectified linear unit – лінійний випрямовувач;

SGD - stochastic gradient descent – стахостичних грідієнтний гасій;

LFR – Live Facial Recognition;

2D-CNN – двовимірна CNN.

АНОТАЦІЯ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет інформаційних технологій
Кафедра технологій управління
Спеціальність 122 - Комп'ютерні науки,
освітня програма «Інформаційна аналітика та впливи»
на кваліфікаційну роботу на здобуття

Дипломна робота магістра Мудрої Анастасія Денисівна.

Тема роботи: «Дослідження залежності зовнішності злочинців від виду скоєного ним злочину методами машинного навчання»

Мета дипломної роботи - створити алгоритм для визначення ступеня залежності між зовнішністю злочинця та виду його правопорушення для вдосконалення загальної точності розпізнавання обличчя та інших цілей.

Об'єктом дослідження є процеси пошуку схожості певного обличчя до певного виду скоєного злочину.

Предметом дослідження є інформаційні засоби, технології, моделі управління даними і процесами при пошуку схожості певного обличчя я до певного виду скоєного злочину.

Наукова новизна одержаних результатів – новий погляд на проблему, що описується, намагається пов'язати зовнішність злочинця з видом його злочину. Це може підвисити точність та прискорити час подальшого розпізнавання обличчя у LFR, через те, що початкова обробка буде здійснюватися по певним рисам обличчя, характерним певним правопорушникам. Також, використання як шаблону для розробки фотороботів.

У роботі досліджується основні тенденції, стан та проблеми сьогоденного розпізнавання обличчя, а також методи, засоби та математичні моделі РО. База даних складається з 1000 фотографій правопорушників та законопорядних людей, де фотографії перших взяті з відкритих джерел FBI

та Interpol. На основі датасету було побудовано програму пошуку збіжностей обличчя із рисами зовнішності правопорушників у real-time за допомогою згорткової нейронної мережі та таких засобів як, python, keras, tensorflow та ін.

Робота складається з наступних розділів: вступ, постановка задачі та аналізу рішення, концептуалізація інформаційного забезпечення дослідження методами машинного навчання, побудови моделі прогнозування скоєного злочину по зовнішності з використанням інформаційного забезпечення, розробки інформаційного забезпечення прогнозування скоєного злочину по зовнішності та рекомендації щодо його використання, висновки, додатки. Всього 90 сторінок, 51 джерело.

Ключові слова: розпізнавання обличчя, правопорушник, згорткова нейронна мережа, TensorFlow, live facial recognition.

ВСТУП

Актуальність теми. Сучасний світ розвивається дуже швидко. Люди стають все більш освіченими та крокують у сторону прогресу та розквіту. Прогрес змінює суспільство на краще, намагається зробити життя людей якомога більш безпечним та комфортним. Але немає нічого у світі, що несе тільки користь. Прогрес також підвищив вимоги до людей. Наприклад, нескінченне навчання протягом життя, велика кількість виборів кожного дня, швидка адаптація та висока екстравертність. Усе це, та багато іншого, несе людині стрес, перенасичення та вигорання. Та кожний вирішує свої проблеми як може. Але найефективніший спосіб, що існує на даний час є психологічна допомога. Зокрема класифікація є дуже вживаною технікою у психології. Отож, основна ідея даної роботи полягає в тому, щоб представити через дослідження залежність між схильністю до певних дій, якою в нашому випадку є вид правопорушення, і зовнішнім виглядом, зокрема, обличчям.

Чому було вирішано взяти саме цю групу населення для проведення дослідження? Бо вона є утрируваною версією психологічних особливостей.

Актуальність теми полягає у допомозі психологам у роботі з різними людьми через дослідження особливостей їх психіки через певні риси обличчя. Чому саме зовнішність? Все більше досліджень пов’язують зображення обличчя з особистістю. Встановлено, що люди здатні з певним ступенем точності сприймати певні риси особистості на обличчях один одного. Дослідження, присвячені об’єктивним характеристикам людських обличь, виявили певні асоціації між морфологією обличчя та рисами особистості. Наприклад, симетрія обличчя передбачає екстраверсію. І, власне, я намагаюсь встановити зв’язок між особою та типом правопорушення, оскільки існує широкий спектр різних видів злочинів, які вимагають від нападника різних ознак і мають різний вплив на потерпілого.

Важливо також зазначити новизну у класифікації та прогнозування за допомогою згорткової нейронної мережі.

Та це не єдине застосування. Криміналісти також використовують таку науку як фізіогноміка. Фізіогноміка - методика виявлення потенціалу, особливостей психіки і поведінки за формою, виразності положенню рис обличчя і їх комбінацій. Вона має не дуже широке використання і є лише набором гіпотез, однак криміналісти у різні часи після винаходу фотографії стали помічати схожі риси в фотокартках злочинців, зроблених після арешту. Стали помічати, що злочинців об'єднують спільні риси обличчя, за якими їх можна було б віднести до правопорушників. Зараз, за допомогою можливостей штучного інтелекту, люди можуть підтвердити або остаточно спростувати цю теорію. Також фізіогноміка може дати точку опору у пошуку закономірностей, бо вона вже використовує набір правил, за якими класифікує і описує людей.

Нововведення, яке пропонується, це класифікація з урахуванням типу і важкості злочину, що відіграють, на справді, не останню роль.

Мета і завдання дослідження. Метою дослідження є створити алгоритм для визначення ступеня залежності між зовнішністю злочинця та виду його правопорушення. Щоб досягти головної мети необхідно зробити такі завдання:

- визначити та описати предметну область дослідження;
- проаналізувати існуючі рішення;
- дослідити доступні бази даних для дослідження;
- проаналізувати методи для вирішення поставленої задачі;
- проаналізувати засоби для вирішення поставленої задачі;
- визначити вхідні данні для дослідження;
- розробити модель для дослідження;
- візуалізувати отримані результати;
- розробити інтерфейс програми прогнозування.

Об'єкт дослідження. Об’єктом дослідження є процеси пошуку схожості певного обличчя до певного виду скоєного злочину.

Предмет дослідження. Предметом дослідження є інформаційні засоби, технології, моделі управління даними і процесами при пошуку схожості певного обличчя я до певного виду скоєного злочину.

Методи дослідження. Найбільш логічним рішенням для вирішення цієї проблеми є використання можливостей нейронної мережі. Необхідно обробити багато інформації, яка, в першу чергу, містить фотографії злочинців. Це найважча частина для нейронної мережі. При обробці зображень виникає потреба сканувати фотографії з різних ракурсів. Тому було прийнято рішення використовувати згорткову нейронну мережу, успішна робота з зображеннями якої підтверджена. Її архітектура включає 2 основні парадигми: локальне сприйняття та спільні ваги.

Далі цю технологію можна використовувати в системах розпізнавання обличчя. У поєднанні з автоматизованим біометричним програмним забезпеченням ця система здатна ідентифікувати або перевіряти людину, порівнюючи та аналізуючи візерунки, форми та пропорції її рис і контурів обличчя. На відміну від людини, алгоритм комп’ютерного зору не має суб’єктивного «багажу», емоцій, упереджень щодо досвіду, раси, релігії, політичних переконань, досвіду. Не втомлюється, не потребує ні сну, ні їжі. Таким чином, іноді це може допомогти різним спеціалістам покращити свою роботу.

Наукова новизна одержаних результатів. Новий погляд на проблему, що описується, намагається пов’язати зовнішність злочинця з видом його злочину. Це може підвисити точність та прискорити час подальшого розпізнавання обличчя у LFR, через те, що початкова обробка буде здійснюватися по певним рисам обличчя, характерним певним правопорушникам.

Також, використання як шаблону для розробки фотороботів.

Практичне значення одержаних результатів. Висновки з дослідження ні в якому разі не закликають називати когось злочинцем, скоріш це спроба дізнатися, чи є залежність зовнішності та прихильності до певної поведінки об’єктивною. Якщо ж кореляція підтвердиться, то далі ці дані можна використовувати для того, щоб запобігати розвиненню небажаної поведінки. Наприклад це може бути класифікація молоді та подальші бесіди зі психотерапевтом, який, як більш освідчений спеціаліст, може допомогти вирішити якісь внутрішні конфлікти, які людина не помічає, ігнорує чи не має допомоги в їх подоланні.

Також перелік можливих застосувань:

- допомагати зробити фоторобот злочинця;
- відстеження поганих звичок, яка відобразились на обличчі.

Апробація результатів роботи. Автор публікувала тези у конферціях «Information Technology and Implementation» 2020 та 2021 року.

Публікації. Двоє тез: "examination of the dependence between criminal's appearance and his offense using machine learning" та "description of the stages of examination a dependence between criminal's appearance and their offense with convolutional neural network"

Структура та обсяг роботи. Магістерська робота складається зі вступу, 4 розділів, висновків, списку використаних джерел з 51 найменувань та додатків. Загальний обсяг курсової становить 90 сторінок, 27 рисунків.

РОЗДІЛ 1. ПОСТАНОВКА ЗАДАЧІ ТА АНАЛІЗ РІШЕННЯ

1.1 Визначення предметної області магістерської роботи

Як було зазначено у вступі, предметна область даної роботи - це перетин розпізнавання обличь та криміналістики. Опишемо кожну з них більш детально.

Розпізнавання обличчя говорить само за себе – це комп'ютерна технологія, що дозволяє ідентифікувати індивідуума за допомогою його цифрової фотографії. Оскільки ця комп'ютерна технологія біометричного порівняння в більшості країн все ще знаходиться на початковому етапі, стандарти та найкращі методи все ще знаходяться в процесі створення. Наприклад, поліція використовує розпізнавання обличь, щоб порівняти фотографії підозрюваних із фотографіями та зображеннями водійських прав. За оцінками, майже половина дорослих американців – понад 117 мільйонів людей станом на 2016 рік – мають фотографії в мережі розпізнавання обличь, яку використовують правоохоронні органи. Тут треба поговорити про неточність алгоритму в залежності від раси. Для подібної технології це швидко переходить у дискримінацією [5].

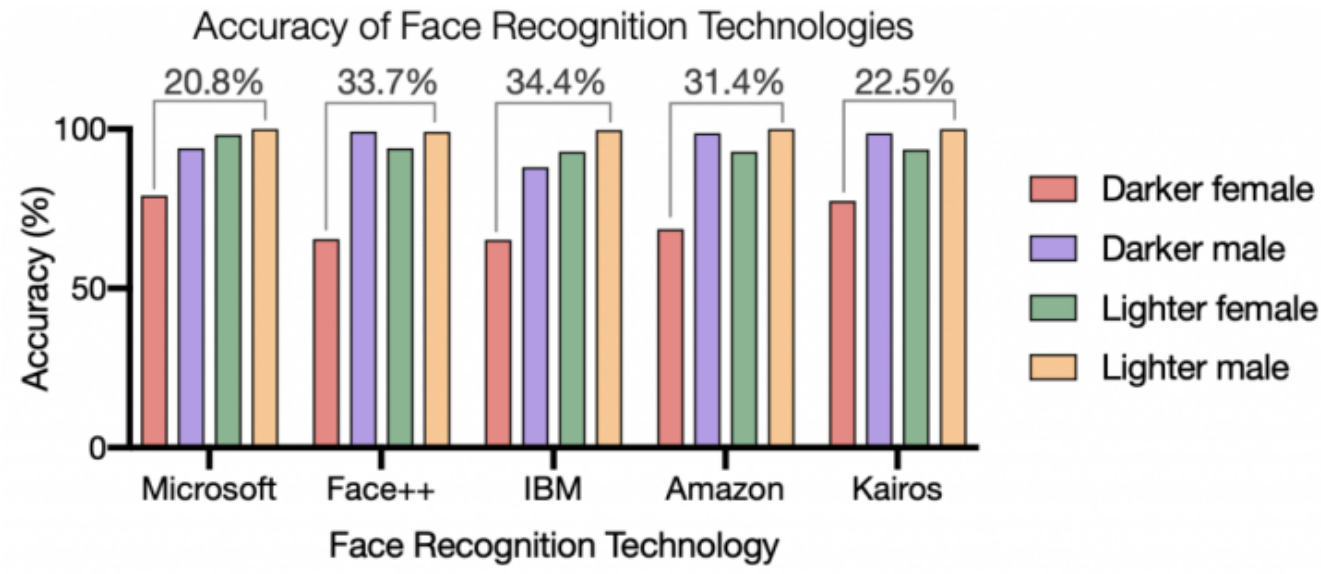


Рис. 1.1. Расова дискримінація у РО

Також показав расову упередженість по відношенню до темношкірих жінок (31% помилка в гендерній класифікації) і Rekognition від Amazon. Цей результат підтвердив попередню оцінку можливостей Rekognition зіставляти обличчя, проведену Американським союзом громадянських свобод, в якій 28 членів Конгресу, непропорційно кольорових людей, були неправильно зіставлені із зображеннями фотографій. Оскільки Amazon продав свою технологію правоохоронним органам, ці розбіжності викликають занепокоєння. Компанії, які надають ці послуги, несуть відповідальність за те, щоб вони були справедливими – як у своїх технологіях, так і в застосуванні. Тому можно переконливо говорити, що область жадає нових підходів та експериментів для підвищення точності у різних класифікаціях.

Але технологічні помилки не лякають інвесторів у даній сфері. Як прогнозують дослідження, пов'язані з аналізом ринку технологій розпізнавання обличь, ринок буде тільки рости. Обсяг глобального ринку розпізнавання обличь у 2020 році оцінювався в 3,86 мільярда доларів США і, як очікується, з 2021 по 2028 рік зростатиме зі зведеними річними темпами зростання (CAGR) на 15,4% [6].

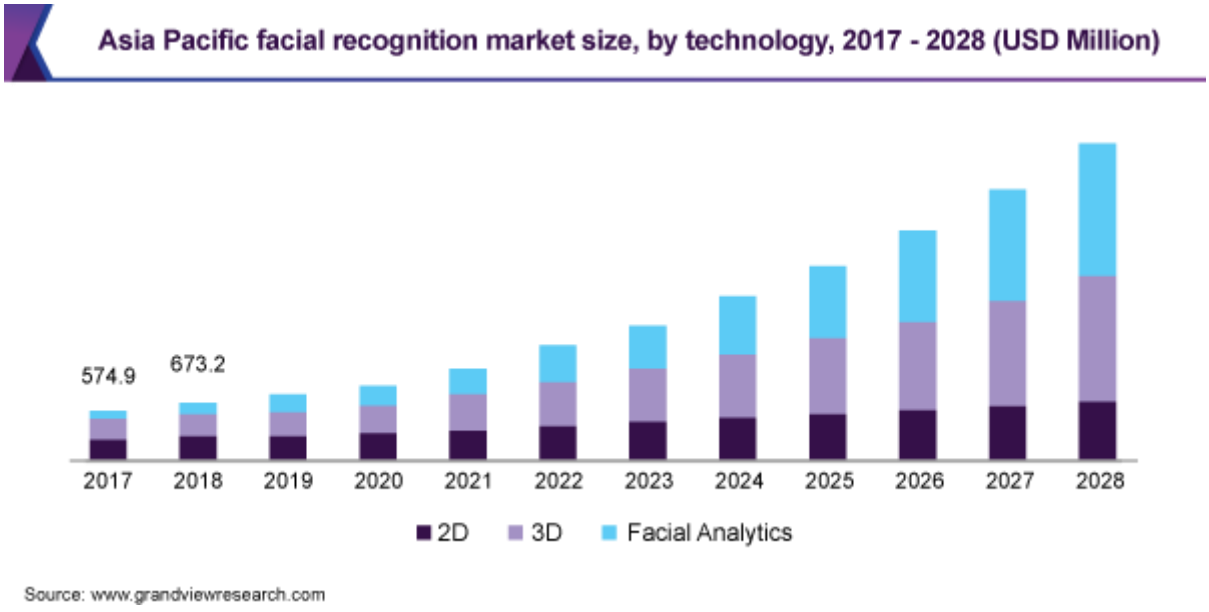


Рис. 1.2. Прогноз роста ринку PO

Технології вдосконалюються, розвиваються та розширюються швидкими темпами. Такі технології, як біометричні дані, широко використовуються для підвищення безпеки. Вони використовуються в різних програмах, таких як контроль доступу, відстеження відвідуваності, безпека та спостереження тощо. Біометрія є універсальною, унікальною та підданою вимірюванню, тому її можна використовувати для забезпечення безпеки. Сьогодні використовуються різні типи біометричних даних, такі як відбиток пальців, розпізнавання райдужної оболонки ока, розпізнавання обличчя, розпізнавання мови та інші. Технологія розпізнавання обличь — це тип технології розпізнавання зображень, який протягом багатьох років отримав широке визнання. Ця технологія використовує підключену або цифрову камеру для виявлення обличь на знятих зображеннях, а потім кількісної оцінки характеристик зображення для відповідності шаблонам, що зберігаються в базі даних.

Також, тут треба зауважити, що навіть Інтерпол використовую у своїй роботі розпізнавання обличчя. Система містить зображення обличь, отримані з більш ніж 179 країн, що робить її унікальною глобальною базою даних про злочини. У поєднанні з автоматизованим біометричним програмним забезпеченням ця система здатна ідентифікувати або перевіряти людину, порівнюючи та аналізуючи візерунки, форми та пропорції її рис і контурів обличчя.

Але і Інтерпол натякає на складнощі у ідентифікації []. На відміну від відбитків пальців і ДНК, які не змінюються протягом життя людини, система має враховувати різні фактори, такі як:

- старіння;
- пластична хірургія;
- косметика;
- наслідки зловживання наркотиками або куріння;
- поза суб'єкта;

- та ін.

Також дуже важливо працювати з якісними зображеннями. Ідеальною була б стандартна фотографія на паспорт, оскільки це фронтальне зображення об’єкта з рівномірним освітленням на обличчі та нейтральним фоном.

Також робота перетинається з криміналістикою. Найчастіше, розпізнавання обличчя використовується в криміналістиці для встановлення особи підозрюваного. Розпізнавання обличчя може бути виконано людиною, штучним інтелектом (ШІ) або обома. Коли робота завершується за допомогою ШІ, основний процес зазвичай включає наступні кроки:

- зображення фіксується;
- комп’ютерна програма бере інформацію про обличчя та перетворює її в цифрову інформацію, наприклад, вимірює простір між очима, форму підборіддя та довжину носа;
- для порівняння тестового обличчя та інших у базі даних використовується спеціальний алгоритм;
- програма визначає, чи відповідає обличчя будь-якому в базі даних.

Друга найважливіша роль у криміналістиці, це реконструкція обличчя. Реконструкція обличчя використовується, щоб спробувати зробити фоторобот правопорушника. Це можна зробити за допомогою тривимірної реконструкції, яка використовує маркери для формування приблизної реконструкції, або двовимірної реконструкції, яка використовує фотографію та ескіз, щоб спробувати створити приблизну реконструкцію.

Досі не існує жодної операційної системи, яка б автоматично порівнювала зображення підозрюваного з базою даних фотографій і надати результат, який можна використовувати в суді. Справа в тому, що біометричне розпізнавання обличчя може в більшості випадків використовуватися для криміналістичних цілей вірно, але питання пов'язані

з інтеграцією технологій з правовою системою суду ще потрібно вирішити. []. Робимо висновок, що автоматизація зараз на достатньо низькому рівні в більшості країн.

Наразі існують деяка автоматизація к питаннях розпізнавання обличчя із фактором старіння обличчя, слідів на обличчі, криміналістичне розпізнавання ескізів, розпізнавання обличь у відео, розпізнавання обличчя ближнього інфрачервоного випромінювання [7].

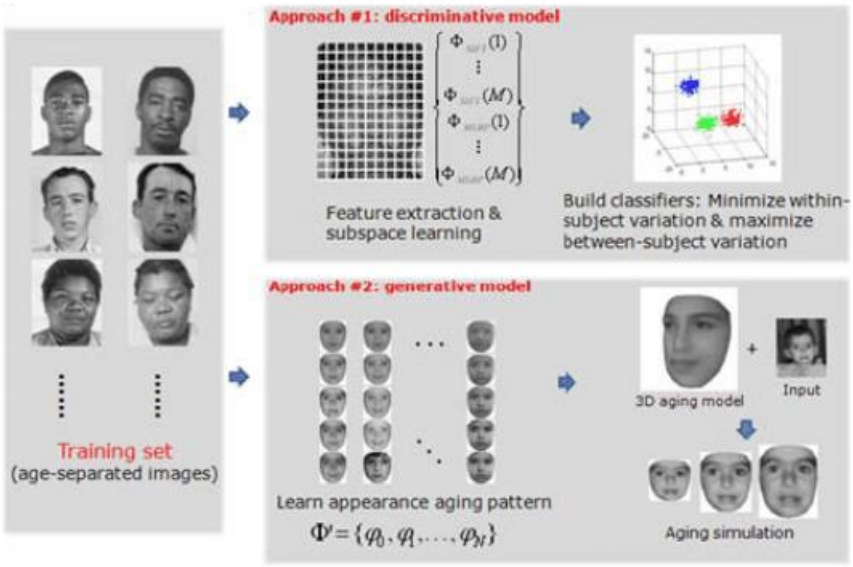


Рис. 1.3. Ілюстрація роботи із старінням у РО

Зазначу прогрес у автоматизації розпізнавання обличь із фактором віку. Старіння обличчя – це складний процес, який впливає як на форму, так і на текстуру (наприклад, тон шкіри або зморшки) обличчя. Цей процес старіння також проявляється в різних проявах у різних вікових групах. Хоча старіння обличчя в першу чергу представлено зростанням обличчя в молодших вікових групах (≤18 років), воно здебільшого характеризується відносно великими змінами текстури та незначними змінами форми (наприклад, через зміну ваги суб'єкта або жорсткості шкіри) у старших вікових групах. (>18 років). Зовнішній вигляд обличчя змінюється більш різко в молодшому віці. Крім старіння обличчя, існують інші фактори, які

впливають на зовнішній вигляд обличчя (наприклад, поза, освітлення, вираз, оклюзія), що ускладнює вивчення моделі старіння.

Отож, популярність використання машинного навчання у різних сферах, в тому числі і в криміналістиці, говорить о доцільності дослідження зовнішності правопорушника. Також, необхідно зазначити, що область зараз знаходиться у стадії досліджень, що робить додаткову цінність проведення поточного експерименту.

1.2 Аналіз існуючих у світі способів її вирішення

В бізнесі розпізнавання обличь є розповсюдженою практикою, але, поки, не має великої точності. Якщо задача ускладнюється якоюсь класиівкацією, то точність наразі падає далі. Якщо говорити про точні аналоги роботи, що проводиться в данній роботі, то їх небагато:

- Rekognition AWS, що мав скандал за неточність алгоритмів [14];
- китайське дослідження, що не вийшло за рамки наукової роботи [1].

Amazon Rekognition — це служба, яка дозволяє легко додавати потужний візуальний аналіз до ваших програм. Rekognition Image дозволяє легко створювати потужні програми для пошуку, перевірки та впорядкування мільйонів зображень. Rekognition Video дозволяє витягувати контекст на основі руху із збережених або прямих відео та допомагає аналізувати їх.

Rekognition Image — це служба розпізнавання зображень, яка розпізнає об’єкти, сцени та обличчя; витягує текст; впізнає знаменитостей; і визначає невідповідний вміст у зображеннях. Він також дозволяє шукати та порівнювати обличчя. Rekognition Image засновано на тій самій перевіреній, високомасштабованій технології глибокого навчання, розробленій вченими Amazon з комп’ютерного зору для щоденного аналізу мільярдів зображень для Prime Photos.

Rekognition Image використовує глибокі моделі нейронної мережі для виявлення та позначення тисяч об’єктів і сцен у ваших зображеннях, і ми постійно додаємо нові мітки та функції розпізнавання обличчя до служби. З Rekognition Image ви платите лише за зображення, які аналізуєте, і метадані обличчя, які ви зберігаєте.

Rekognition Video — це служба розпізнавання відео, яка виявляє дії; розуміє переміщення людей у кадрі; і розпізнає об’єкти, знаменитостей і невідповідний вміст у відео, що зберігаються в Amazon S3, і прямих відеопотоках від Acuity. Rekognition Video виявляє людей і відстежує їх через відео, навіть якщо їх обличчя не видно, або коли вся людина може входити та виходити з місця події. Наприклад, це можна використовувати в програмі, яка надсилає сповіщення в режимі реального часу, коли хтось доставляє посилку до ваших дверей. Rekognition Video також дозволяє індексувати метадані, такі як об’єкти, дії, сцени, знаменитості та обличчя, що полегшує пошук відео [14].

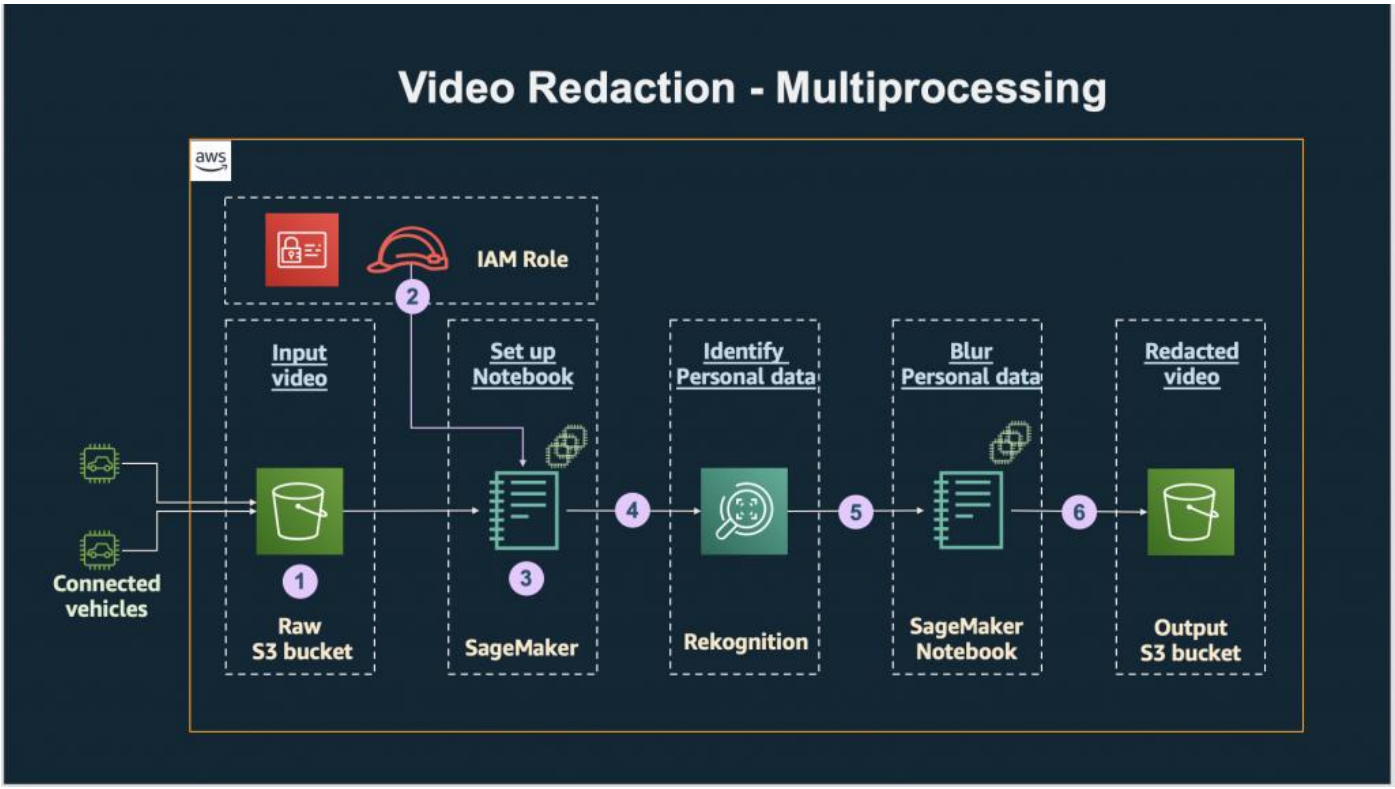


Рис. 1.5. Ілюстрація архітектури AWS Rekognition

Responses to Critiques on Machine Learning of Criminality Perceptions. Вперше було розроблено систему, що може робити автоматизований висновок про злочинність, заснований виключно на нерухомих зображеннях облич, які не містять будь-яких упередженнь та суб'єктивних суджень людей-спостерігачів.

У статті описується, як із допомогою машинного навчання чотири класифікатори(логістична регресія, KNN, SVM, CNN) із використанням зображень обличь 1856 реальних осіб, різні за расою, статтю, віком та мімікою, майже половина з яких була засуджена як злочинці, за розрізнення злочинців і незлочинців. Усі чотири класифікатори працюють стабільно добре і емпірично встановити обгрунтованість автоматизованого обличчя-індукованого висновока про злочинність, незважаючи на історичні суперечки навколо цієї лінії розслідування. Крім того, були визначені деякі відмінні структурні особливості для прогнозування злочинності, що знайдено за допомогою машинного навчання. Перш за все, найважливішим відкриттям цього дослідження є те, що кримінальні і некримінальні зображення обличь мають два досить відмінні різновиди. Різниця між особами злочинців значно більша, ніж між тими, хто не є правопорушниками. Два різновиди, що складаються з кримінальних і не-злочинних осіб, здаються концентричними, причому некримінальний різновид лежить у середині, демонструючи закон «нормальності» для обличчя. Інакше кажучи, обличчя типової нормальної людини має більший ступінь подібності порівняно з обличчями злочинців [2].

Ву та Чжан виявили, що нейронна мережа може ідентифікувати злочинця з точністю до 89,5%.

Головним досягненням вчених, що описується в статті є знаходження за допомогою нейронної мережі трьох рис обличчя, по яким тнейронна мережа може вказати на правопорушника. На відміну від людей правопорядних, злочинці мають на 23,4% більш серивлену верхню губу,

відстань між внутришніми уголками очей меньший на 6%, а кут від носа у трикутнику, що з’єднує очі та рот на 20% менший.

Також, необхідно зазначити деякі роботи, що мають значення для поточного дослідження, через вирішення, хоч і не на перший погляд, схожих проблем:

- Localizing Anomalies from Weakly-Labeled Videos [4];
- Face recognition for criminal identification [3].

Localizing Anomalies from Weakly-Labeled Videos. Виявлення аномалій відео під мітками рівня відео наразі є складним завданням. Вже були роботи, що зробили прогресує до визначення того, чи містить відео аномалії. Однак більшість з них не можуть точно локалізувати аномальні події у відео у часовій області. У статті розказується про метод, зосереджений на тимчасовій локалізації аномалій в аномальних відео.

Запропоновані в статті методи використовуються на гарному датасеті з відео аномалій. Набір даних UCF-Crime — це великомасштабний набір даних із 128 годин відео. Він складається з 1900 довгих і необрізаних відеоспостереження в реальному світі з 13 реалістичними аномаліями, включаючи зловживання, арешт, підпал, напад, ДТП, крадіжку, вибух, бійку, пограбування, стрілянину, вандалізм та інші підкатегорії правопорушень. Ці аномалії обрані, оскільки вони мають значний вплив на безпеку населення. Цей набір даних можна використовувати для двох завдань. По-перше, загальне виявлення аномалій, враховуючи всі аномалії в одній групі та всі нормальні дії в іншій групі. По-друге, для розпізнавання кожної з 13 аномальних дій. В статті наводиться візуалізація передбачення аномальної поведінки на відео.

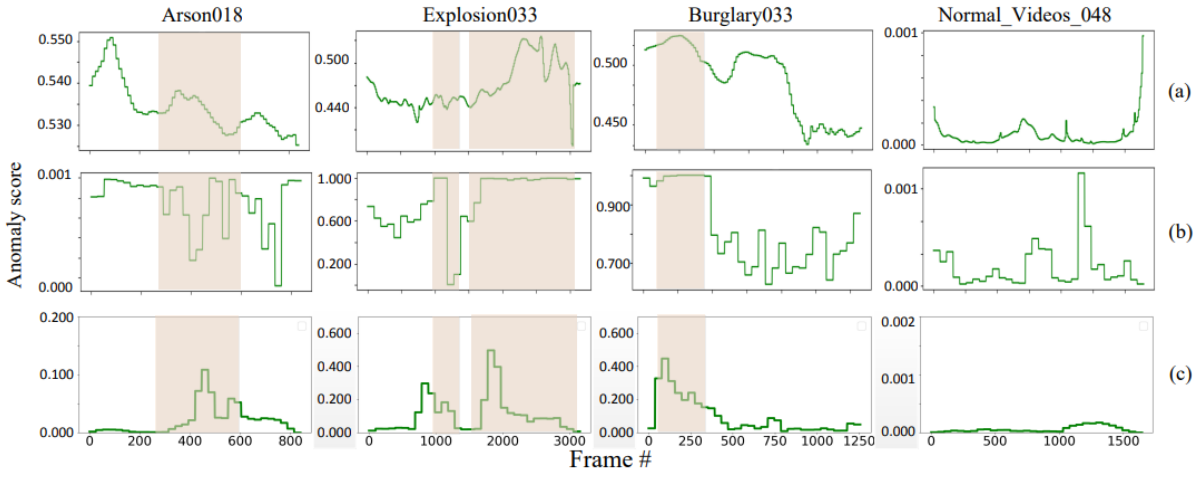


Рис. 1.6. Візуалізація аномалій з відео спостережень

Виявлення аномалій, тобто тих моделей поведінки або зовнішності, які не відповідають звичайним шаблонів має велике значення для сигналізації потенційних ризиків або небезпеки. При широкомасштабному розгортанні спостереження, нагальна вимога інтелектуальних систем полягає в тому, щоб автоматично відфільтрувати можливі ненормальні події.

Як висновок, у статті запропонована локалізації аномалій у відеоспостереження та описано слабко контрольовану мережу локалізації аномалій, яка глибоко досліджує тимчасовий контекст у послідовних сегментах. Додатково, модель тимчасової динаміки варіації, а також семантична інформація високого рівня. Точність локалізації аномалії була значною покращено після запровадженого зменщення шуму відео. Не має сумніву, що запропонований детектор аномалій працює значно краще, ніж попередні методи.

Face recognition for criminal identification: An implementation of principal component analysis for face recognition. В цій роботі, в першу чергу, цікаво, що алгоритм розробляється для ідентифікування певних неоднотипних рис обличчя.

Протягом багатьох років було розроблено немало підходів до безпеки, які допомагають зберегти конфіденційні дані і обмеження

ймовірності порушення безпеки. Алгоритм, що описується наступний. Розпізнавання обличь для ідентифікації злочинців — це система розпізнавання, в яку експерт з безпеки вводить зображення відповідної особи всередині системи, і система спочатку обробить зображення, тобто виключить небажані елементи, такі як шум. Після цього система класифікує зображення на основі своїх орієнтирів, наприклад, відстані між очима, довжини лінії щелепи тощо. Потім система виконає пошук у базі даних, щоб знайти ідеальну відповідність і відобразити вихідні дані. Ця робота зосереджена на впровадження системи виявлення злочинців. Сучасна практика ідентифікації відбитків великого пальця, яка є простою у реалізації, але іноді неможливо отримати відбитки з місця злочину. Злочинці стали розумнішими і зазвичай дуже обережні, залишаючи будь-який відбиток пальця на місці події. Ця система охоплювала базу даних обличь і алгоритм обробки зображень, щоб узгоджувати стрічку обличь із збереженими обличчями в базі даних.

Найважливіші кроки в системі можуть бути класифіковані на чотири основні категорії:

- методи обробки інформації;
- інваріантні ознаки;
- знаходження шаблонів;
- інформація на основі зовнішнього вигляду.

Для визнання необхідні два етапи. Процес навчання та процес оцінювання. У процесі навчання алгоритм отримує зразки зображень, які потрібно вивчити і під час процесу оцінювання для кожного зображення визначається модель нещодавно отриманого зображення, що порівнюється з усіма існуючими в базі даних. Потім проводиться перевірка, чи спрацювало розпізнавання. На цьому етапі проводиться статистична процедура, аналіз основних компонентів, що використовується для набору зображень обличь

для формування набору базових ознак, які називаються набором власних ознак. Мета дослідження двояка:

- точне узгодження обличчя з наявною базою даних;

- застосування аналізу головних компонентів для пошуку відмінних рис серед багатьох зображень, щоб отримати їх схожість для цільового зображення.

1.3 Аналіз методу розпізнавання обличчя правопорушника

А. Стадія ранньої алгоритмізації. У 1950-х роках люди почали вивчати, як змусити машини розпізнавати обличчя. У 1964 році офіційно почалися прикладні дослідження інженерії розпізнавання обличчя, в основному з використанням геометрії обличчя для розпізнавання. Але на практиці він не застосовувався.

1) Аналіз основних компонентів. Principal component analysis (PCA)

Аналіз головних компонентів (PCA) є найбільш широко використовуваним алгоритмом зменшення розмірності даних. В алгоритмах розпізнавання обличчя PCA реалізує вилучення ознак обличчя. У 1991 році Терк і Пентленд з Медіа-лабораторії Массачусетського технологічного інституту ввели аналіз основних компонентів у розпізнавання обличь [5]. PCA зазвичай використовується для попередньої обробки даних перед іншими аналізами. У зовнішніх даних із більшими розмірами він може видалити зайву інформацію та шум, зберегти основні характеристики даних, значно зменшити розміри, підвищити швидкість обробки даних та заощадити багато часу та коштів. Тому цей алгоритм зазвичай використовується для зменшення розмірності та візуалізації багатовимірних даних.

В алгоритмах виділення ознак на основі PCA, власна грань є одним із класичних алгоритмів. На малюнку 2 показано простий процес виділення ознак, де PCA поєднується з розпізнаванням обличчя за допомогою

алгоритму K-Nearest-Neighbor (KNN). Ми отримуємо власні значення та власні вектори коваріаційної матриці з даних вибірки та вибираємо головний компонент, який є власним вектором з найбільшим власним значенням. У той же час матриця ознак даних тестування отримується тим самим процесом зменшення розмірності. Нарешті, категорія зображення обличчя тестового набору виявляється класифікатором KNN. Хоча PCA ефективний у роботі з великими наборами даних. Його найбільшим недоліком є те, що його навчальний набір даних має бути достатньо великим. Наприклад, кількість оригінальних фотографій у системі розпізнавання обличь має бути не менше тисячі, тому результати аналізу основних компонентів мають значення. Однак, коли вираз обличчя людей відрізняється, є перешкоди, які блокують обличчя, або світло занадто сильне або надто слабке, і важко отримати хороші малорозмірні дані.

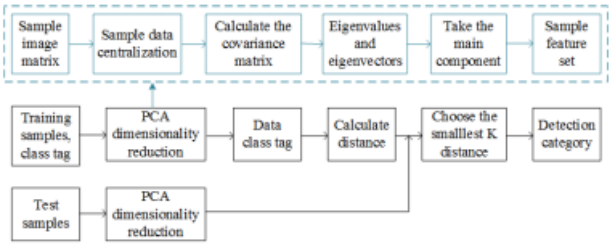


Рис. 1.7. Алгоритм PCA

2) Лінійний дискримінантний аналіз. Linear discriminate analysis (LDA)

Для набору даних розпізнавання обличчя з мітками ми можемо використовувати лінійний дискримінаційний аналіз (LDA). Він використовується для класифікації обличчя. PCA вимагає, щоб дисперсія даних після зменшення розмірності була якомога більшою, щоб дані можна було розділити якомога ширше, тоді як LDA вимагає, щоб дисперсія в межах тієї ж категорії груп даних після прогнозування була якомога меншою, а дисперсія між групами, щоб бути якомога більшими. Це означає,

що LDA наглядає за зменшенням розмірності і має використовувати інформацію мітки для розділення різних категорій даних якомога більше.

Б. Штучні риси та стадія класифікації

1) Метод опорних векторів. Support vector machine (SVM)

У 1995 році Вапнік і Кортес запропонували метод опорних векторів (SVM) [13]. Метод опорного вектора — це алгоритм, спеціально розроблений для задачі розпізнавання обличчя з невеликою вибіркою. Це класифікатор, розроблений на основі узагальненого портретного алгоритму. Завдяки своїй відмінній продуктивності в класифікації текстів вона незабаром стає основною технологією машинного навчання. У розпізнаванні обличь ми використовуємо виділені риси обличчя та SVM, щоб знайти гіперплощину для розрізнення різних обличь. Припустимо, що існує двовимірний простір з багатьма навчальними даними. SVM повинен знайти набір прямих ліній, щоб правильно класифікувати навчальні дані. Через обмеження кількості навчальних даних вибірки поза навчальним набором можуть бути ближче до лінії сегментації, ніж дані в навчальному наборі. Тому ми вибираємо лінію, найбільш віддалену від найближчої точки даних, а саме опорний вектор. Такий метод сегментації має найсильнішу здатність до узагальнення, як показано на рис 1.8.

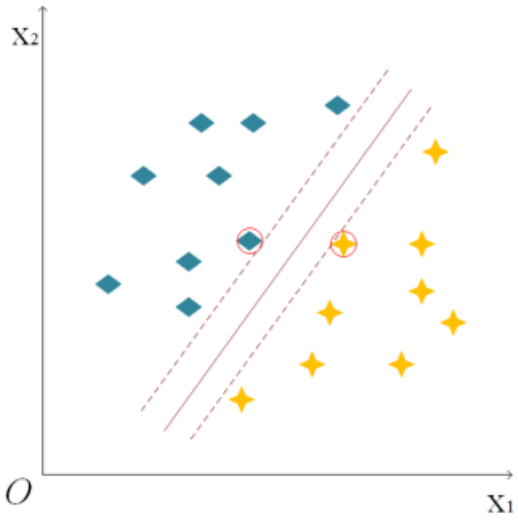


Рис. 1.8. Опорний вектор

Зазначений вище метод розрізняє дані на двовимірній площині, але ця теорія також може бути застосована до тривимірного або навіть більшого простору, лише межа, яку потрібно знайти, стає площиною або гіперплощиною.

2) Adaboost

Оригінальний алгоритм бустінгу був запропонований Шапіром [15]. Використовується для розпізнавання обличчя. Алгоритм бустінгу може підвищити точність будь-якого даного алгоритму навчання. Основна ідея полягає в тому, щоб інтегрувати різні класифікатори в сильніший остаточний класифікатор за допомогою деяких простих правил, щоб загальна продуктивність була вищою. Є дві проблеми для розпізнавання обличчя в алгоритмі бустінгу. Одне – як налаштувати навчальний набір, а інше – як ідосконалити слабкий класифікатор, щоб сформувати сильний класифікатор. Adaboost покращив ці проблеми, і було доведено, що він є ефективним і практичним алгоритмом підвищення рівня розпізнавання обличь. Adaboost використовує зважені навчальні дані замість випадково вибраних навчальних вибірок, щоб зосередитися на відносно складних вибірках навчальних даних. Adaboost використовує механізм зваженого голосування замість механізму середнього голосування, тому слабкий класифікатор з хорошим ефектом класифікації має більшу вагу. Класифікатор Adaboost можна розуміти як функцію. Він вводить значення характеристики x і повертає значення G(x). У класифікаторі adaboost кілька слабких класифікаторів Gi об'єднані в сильний класифікатор, і кожен слабкий класифікатор має вагу wi , що показано таким чином G(x) = sign(Xn i=1 wi ∗ G(xi)) У розпізнаванні обличчя , за допомогою алгоритму adaboost слід використовувати характеристики Хаара для кожного зображення. Ця особливість відображає зміну рівня сірого зображення.

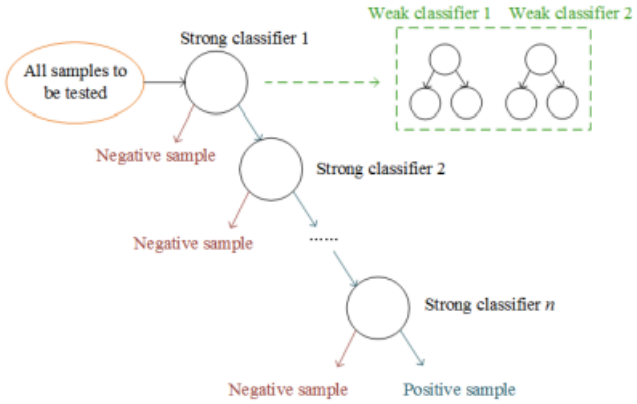


Рис. 1.9. Алгоритм Хаара

Класифікатор Хаара є каскадним застосуванням алгоритму adaboost [19]. Структура каскадного класифікатора показана на рис. 6. Кожен каскадний класифікатор містить кілька слабких класифікаторів, і структура кожної слабкої класифікації також є деревом рішень.

3) Маленькі виборки

Проблема малої вибірки пов’язана з тим, що кількість навчальних вибірок для розпізнавання обличчя занадто мала, що призводить до того, що більшість алгоритмів розпізнавання обличчя не досягають своєї ідеальної продуктивності розпізнавання. Для того, щоб ефективно зберігати інформацію про зображення, підтримувати зв’язок між зразками, зменшувати вплив шуму та ще більше посилювати ефект розпізнавання обличчя, було проведено багато досліджень. Хоуланд та ін. запропонував метод, який поєднує лінійний дискримінантний аналіз із узагальненим розкладом сингулярних значень (GSVD) для вирішення проблеми розміру вибірки [P. Howland, J. Wang, and H.]. Він та ін. представив спосіб покращення ефективності методів лінійного дискримінантного аналізу на малих вибірках за допомогою процесу декомпозиції Хаусхолдера QR у різних просторах [Y. He, ‘‘An efficient method to]. Ці дослідження значно покращили ефективність розпізнавання обличь.

4) Нейронні мережі

Нейронна мережа – це алгоритм, призначений для моделювання людського мозку для розпізнавання обличчя. Розпізнавання обличь, як один із найбільш актуальних методів розпізнавання для біометричних даних, став одним із дослідницьких фокусів у галузі нейронних мереж.

Нейрон типової нейронної мережі складається з лінійної функції та нелінійної функції активації, як показано на рис 1.10.

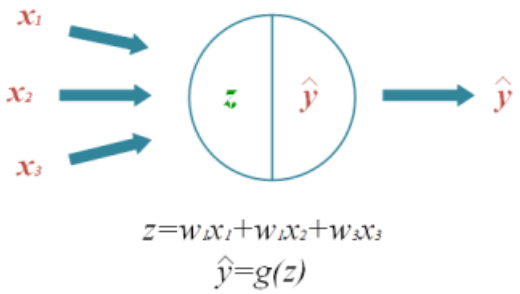


Рис. 1.10. Малюнок нейрона

Нейрон нейронної мережі. Лінійна функція тут відноситься до того, що кожен нейрон пов’язує переданий сигнал з вагою (z(x) = wx + b), тоді як функція активації має справу з виходом нейрона. Ідеальна функція активації відобразить результат на «0» або «1». На початку сигмовидна функція була більш популярною, і вона може стиснути вихід у великому діапазоні в діапазоні [0, 1]. Зараз найбільш часто використовуваною функцією є випрямлена лінійна одиниця (ReLu) [44].

1.4 Визначення вхідних даних для вирішення поставленої задачі

У ході експерименту будуть використана деяка кількість вхідних даних. Вони представляють собою фотографії злочинців з різних сайтів безпеки. Також вибірка складає собою людей з різними злочинами за спиною.

Бази даних злочинців є в кожній країні, але вони знаходяться під захистом. Тому перша інформація для моделі подається від Інтерполу з категорії «Червоні мітки». Червоні мітки видаються втікачам, які розшукуються або для притягнення до відповідальності, або для відбування покарання. Червона мітка— це запит до правоохоронних органів у всьому світі з проханням знайти та тимчасово заарештувати особу, яка очікує екстрадиції, видачі чи подібних судових позовів. Природно, що набір даних потребує додаткових доповнень. Необхідно повторити експеримент з більшою кількістю людей різного віку, статі, етнічних груп і з більшою інформацією про них, як мотиви. Обгрунтую одну важливу річ, чому були обрані саме ці категорії правопорушень. Головна ідея полягає в тому, що різні образи поведінки спроваковані різними особливостями психіки, та, як ми досліджуємо, зовнішності. Опишемо кожний клас більш детально.

Вбивці. Здатність психопатів обманювати, брехати та маніпулювати означає, що їхня потенційна небезпека для інших може не бути оцінена органами кримінального правосуддя, тому що їхня реакція на клінічну оцінку часто фальсифікована, і тому що дослідники не бачать основних мотивів. Зіткнувшись із проблемою виявлення соціально стигматичних переконань, психологи досі шукають спосіб виміряти їхні психологічні особливості.

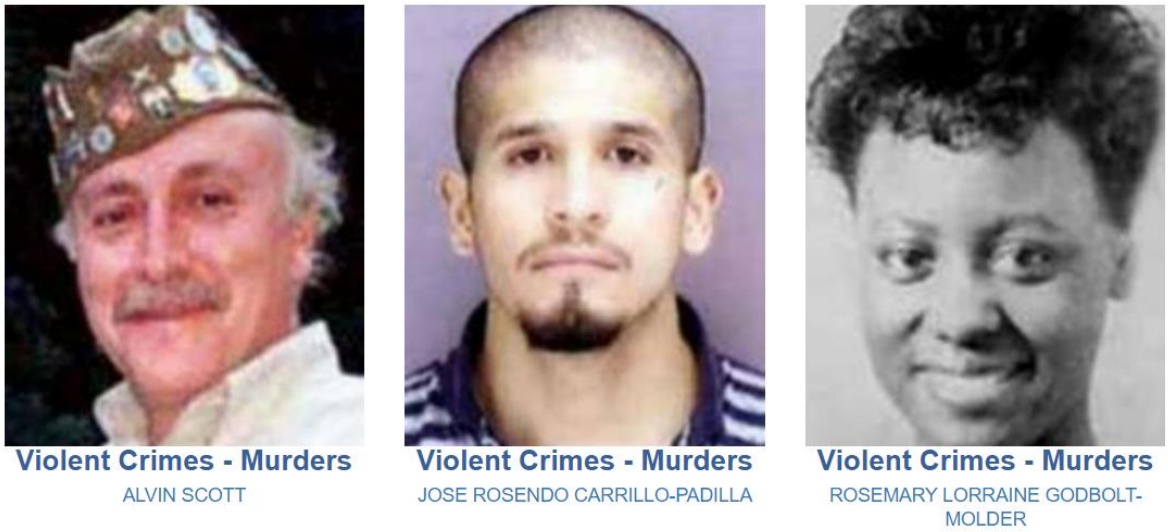


Рис. 1.11. Візуалізація датасету

Отже, що можна сказати про причини скоєння вбивства, коли існує так багато видів вбивств? «Мотив» є центральним для поліційського розслідування. Хоча засудження можливе без виявлення мотиву, знаходження конкретгої причини робить набагато більш вірогідним розкриття певної справи.

Умовно мотиви вбивство можна звести до чотирьох наборів:

- страсть;
- любов;
- ненависть;
- вигода.

Страсть: закоханий вбиває суперника заради свого бажання. «Вбивця гострих відчуттів», який вбиває людей, тому що отримує сексуальну винагороду.

Кохання: «вбивство з милосердя» дитини з деформацією або партнера з невиліковним раком.

Ненависть: смертельна ненависть, спрямована до однієї людини (наприклад, образливий батько), група (наприклад, гомосексуалістів чи

повій), культури чи нації (для наприклад, палестинці по відношенню до ізраїльтян і навпаки).

Вигода: вбивство з метою отримання фінансової вигоди через спадщину або страхові виплати; вбивство, що сталося під час пограбування, або бандитська війна за контроль над ринки наркотиків. Працевлаштування вбивцею на замовлення або найманець.

Однак переважна більшість людей не бере на себе зобов'язань вбивство та не розуміють усіх наслідків.

Крадії банків. Очевидно, що банки та кредитні спілки є мішенню для пограбування. Ось де гроші. Пограбування відбуваються щодня, Google каже, що нове сталося лише дві години тому. Більшість із них передбачає передачу касиру простої записки. Насильство трапляється рідко, але воно буває.

Незважаючи на те, що кількість викрадених грошей зазвичай невелика, потенційна загроза для співробітників і клієнтів залишається високою. Міністерство юстиції США каже, що коли відбувається пограбування, люди нормально реагують на ненормальну подію, часто зі страхом, провиною, гнівом і депресією.

Терористи. Тероризм може відбуватися в різних формах і випадках. Терористи можуть бути обділеними, неосвіченими, заможними та представниками обох статей. Це може відбуватися в розвинених і нерозвинених країнах, у різних режимах. Він охоплює ідеологію та релігію. Хоча те, що породжує тероризм, може відрізнятися від того, що з часом продовжує тероризм.

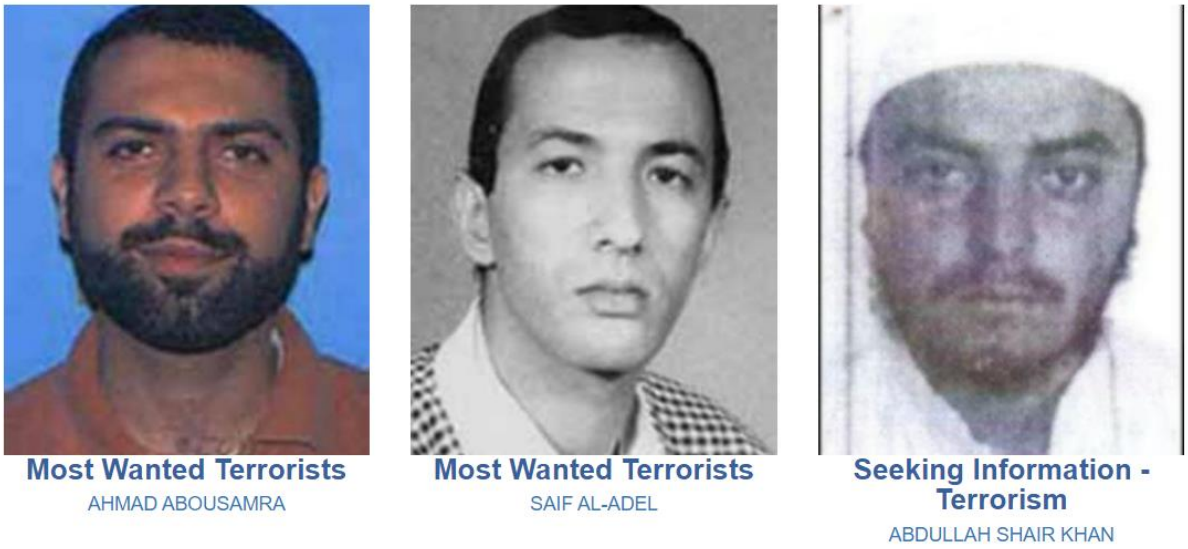


Рис. 1.12. Візуалізація датасету

Суспільства, які більше піддаються впливу, як правило, такі:

- бідні суспільства зі слабкими державними структурами. Вони більше схильні до громадянських воєн, ніж заможніші країни, і, отже, зростає ризик тероризму.
- держави, залучені до демократичного перехідного періоду, а не до демократичних чи авторитарних режимів. Рівень транснаціонального тероризму найвищий у напівавторитарних державах.
- зазнає суспільних змін, спричинених модернізацією. Таким чином створюються умови для тероризму через мобільність, комунікацію, широке поширення цілей і аудиторії.
- слабкі та розпалені держави, які сприяють міжнародному тероризму. Поточні або минулі війни можуть мати терористичні мотиви. Збройні конфлікти також мають сприятливий вплив на транснаціональний тероризм.

Також, будуть добавлені фотографії правопорядних людей, для ідентифікації, чи є людина взагалі злочинцем.

1.5 Висновки до першого розділу

Інкапсулюючи методи, головним завдання дослідження зовнішності злочинця та видом його правопорушення, це знайти закономірності у зовнішності правопорушників, що відповідають певній тяжкості злочину, тому що існує широкий спектр різних видів злочинів, які вимагають різних рис від нападника і мають різний вплив на жертв [1].

В цьому розділі було описано предметну область, що досліджується. Показано, що область потребує подальших вдосконалень та тільки збільшує потік інвестицій. Було описано технології, які наразі використовуються для подібних задач та описана їх точність та наукова цінність.

Також, не забуті і статті, в яких описуються доречні для даної роботи підходи та наукові здобутки. Був проведений аналіз існуючих методів розпізнавання обличь. В ході розділу описано вхідні данні, що використовуються, описані мотиви взяття саме цих даних. Також сформульовано завдання, що виконується у рамках поточного наукового дослідження.

РОЗДІЛ 2. КОНЦЕПТУАЛІЗАЦІЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДОСЛІДЖЕННЯ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

2.1. Методи обробки інформації.

Як було вже висвітлено, основним методом обробки інформації в досліджені зовнішності злочинця від виду скоєного ним злочину буде виступати згорткова нейрона мережа.

Обличчя є основним засобом розпізнавання людини, передачі інформації, спілкування з іншими та визначення почуттів людей, зокрема. Наші обличчя можуть розкрити більше, ніж ми очікуємо. Зображення обличчя може бути інформативним про особистісні риси [1], такі як раса, стать, вік, здоров'я, емоції, психологія та професія.

Це дослідження викликане дослідженням Ломброзо [2], яке показало, що злочинців можна ідентифікувати за структурою обличчя та емоціями. У той час як у дослідженні Ломброзо це питання розглядалося з точки зору фізіології та психіатрії, наше дослідження досліджує, чи зможуть алгоритми машинного навчання вчитися та розрізняти кримінальні та некримінальні зображення обличчя та ідентифікувати його за видом злочином.

Варто відзначити, що обсяг цього дослідження обмежений технічними та аналітичними аспектами цієї теми, тоді як його соціальні наслідки вимагають більш ретельного вивчення, а його практичне застосування вимагає ще більш високого рівня обережності та підозрілості. З огляду на це, ця стаття досліджує здатність глибокого навчання розрізняти кримінальні та некримінальні зображення обличчя. Для цього згорткова нейронна мережа (CNN), навчаються за допомогою 1000 зображень обличчя з нейтральними емоціями, змішаної статі та змішаної раси. Нейтральне або пусте обличчя характеризується нейтральним розташуванням рис обличчя. Нейтральний вираз обличчя може бути викликаний відсутністю емоцій, нудьгою, депресією або легкою розгубленістю. Нейтральний вираз обличчя

також називають покерним обличчям. Він призначений для приховування своїх емоцій під час гри в карткову гру в покер. Хоча модель нейронної мережі контролюються для емоцій обличчя шляхом застосування лише нейтральних зображень емоцій, контроль не накладено на расу через невеликий набір даних, а також через складність, а іноді й суб'єктивність ідентифікації раси за низькоякісними зображеннями обличчя.

Сила цього дослідження полягає в застосуванні нейронних мереж для дослідження, чи може набір нелінійних функцій із тисячами параметрів знайти корисні риси обличчя, щоб розрізнити кадри кримінального та некримінального обличчя. Однак його слабкість полягає в тому, що він покладається на машину для вивчення цих функцій і на обмежену кількість зображень.

Архітектура нейронної мережі

Як показано на рис. 1, дані передаються до штучної нейронної мережі для подальшої класифікації. Штучні нейронні мережі не покладаються на створені вручну функції, які важко вибрати та спроектувати. Нейронна мережа в нашій програмі отримує як вхідні зображення 45×45 пікселів у відтінках сірого. Перш ніж описувати архітектуру нейронної мережі, я обґрунтовую мій вибір функції активації, функції втрат і алгоритму навчання.

У той час як насичені функції активації, напр. sigmoid або tanh, можуть викликати проблему зникаючих градієнтів і запобігти проблемі градієнтів, що вибухають, через їх майже нульовий градієнт при великих значеннях, ненасичені функції активації, напр. випрямлена лінійна одиниця (ReLU), може викликати проблему градієнтів, що вибухають, і запобігти проблемі зникаючих градієнтів через їх відмінний від нуля градієнт при великих значеннях. Обидві проблеми виникають із синаптичними вагами на нижніх шарах і заважають правильному навчанню мережі. Проблему з вибухаючим градієнтом легше виявити, тому що зникнення градієнтів

також може статися через конвергенцію навчання. Крім того, ненасичені функції активації прискорюють навчання в кілька разів [13]. Тому ми обрали ненасичену функцію активації ReLU [27, 28]. ReLU — це кусково-лінійна функція, яка визначається як додатна частина її аргументу: $ReLU(z) = max(0,z)$. Проектуючи негативні вхідні дані до нуля, ReLU створює розрідженість в активації нейронних одиниць, бажаний ефект, подібний до випадання. Функція softmax, $softmax(zi) = exp(zi)/\Sigma j\ exp(zj)$, що використовується в кінцевому шарі, перетворює значення (zi) на нормалізовані експоненційні ймовірності, підсумовування яких дорівнює одиниці (тобто $\Sigma c\ pc = 1$). Це ($\Sigma c\ pc = 1$) є передумовою для застосування функції втрат перехресної ентропії, яка розраховується як: $-\ \Sigma c\ yc\ log(pc)$, де c представляє нейрон (або клас) у вихідному шарі, yc являє собою бажане значення (0 або 1) для цього нейрона, а pc – це передбачена ймовірність для цього нейрона. У нашому випадку функція втрат перехресної ентропії спрощується до $-\ (y\ log(p) + (1 - y)\ log(1 - p))$ для бінарної класифікації. Мережа навчається за допомогою алгоритму оптимізації Adam [29], яке є розширенням підходу стохастичного градієнтного спуску (SGD) з розміром пакету 100. На відміну від SGD, який підтримує єдину і фіксовану швидкість навчання для всіх синаптичних оновлень ваги, Adam постійно коригує індивідуальну швидкість адаптивного навчання для кожної синаптичної ваги на основі оцінок першого та другого моментів градієнтів. Швидкість навчання ініціалізується на рівні 0,0001, а експоненційна швидкість розпаду для оцінок першого та другого моменту встановлюється на 0,9 та 0,999 відповідно, запропоновано Кінгмою та Ба [29].

НМ CNN більше підходить для поточної задачі, хочу це підтвердити невеликим зіставленням із класичною нейронною мережею SNN.

Архітектура нейронної мережі застосовуються для класифікації зображень обличчя на 3 кримінальні групи та некримінальні категорії. CNN нещодавно перевершила інші архітектури нейронних мереж та інші підходи

машинного навчання та обробки зображень у класифікації зображень [13, 30, 31, 32, 33, 34, 35, 36] та виявлення об’єктів [37] завдяки своїй незалежності від ручної роботи. візуальні особливості та чудові абстрактно-смислові здібності [34, 38]. CNN робить сильні і переважно правильні припущення про природу зображень, а саме про локальність піксельних залежності та стаціонарність статистики. Таким чином, у порівнянні з SNN з шарами однакового розміру, CNN має набагато менше з’єднань і параметрів, що полегшує навчання.

У наступних двох абзацах погоаоримо про явні переваги згроткової нейноррної мережі.

Часткове з’єднання, а не повне з’єднання. Вузол в CNN підключений лише до невеликої кількості вузлів попереднього рівня, тоді як той самий вузол у SNN підключений до всіх вузлів попереднього рівня. Це означає, що кількість синаптичних ваг, які необхідно розрахувати, у CNN набагато менше, ніж у SNN. Припустимо, що ми використовуємо вікно згортки 3×3 в CNN, показане зліва на рис. Це означає, що вузол у першому прихованому шарі, наприклад, підключений лише до 9 пікселів зображення. Той самий вузол у SNN, показаний у правій частині рис., підключений до всіх 270 пікселів зображення. Іншими словами, кількість синаптичних ваг у CNN у 30 разів менше, ніж у SNN. Звичайно, це число залежить від розміру як зображення, так і вікна згортки. Якщо зображення дорівнює $n \times m$, а вікно згортки — $z \times z$, кількість синаптичних ваг у CNN у $n \times m/z2$ рази менше, ніж у SNN. Це показано лише для першого прихованого шару, але те саме стосується всіх згорткових прихованих шарів. Це має дві переваги. По-перше, набагато менше невідомих параметрів (синаптичних ваги) можна дізнатися швидше (менша обчислювальна складність) і значно менша ймовірністю перенасичення. По-друге, отримання значення кожного вузла в наступному шарі лише з невеликої кількості сусідніх пікселів, а не з усього зображення,

засноване на припущенні, що зв'язок між двома віддаленими пікселями, ймовірно, менш значущий, ніж двома близькими сусідами. Це припущення навіяно системою зорової кори у людей та інших тварин.

Спільні ваги. Згадувалось, що n × m синаптичні ваги потрібно дізнатися для одного вузла в першому прихованому шарі SNN. Для k вузлів у першому прихованому шарі необхідно обчислити загалом n × m × k синаптичних ваг, оскільки кожен вузол у першому

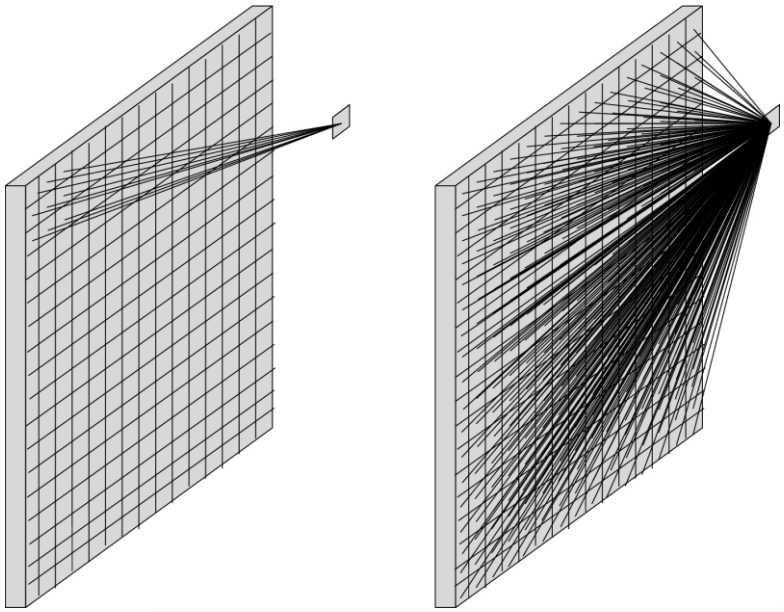


Рис. 2.1. Зіставлення роботи SNN та CNN

прихованому шарі має свої власні синаптичні ваги, які відрізняються від інших вузлів. Однак у CNN кількість синаптичних ваг, які необхідно вивчити, залишається z2, оскільки вузли в першому прихованому шарі не мають різних синаптичних ваг, а мають однакові. Тому, незалежно від того, скільки вузлів існує в першому прихованому шарі, кількість синаптичних ваг, які необхідно вивчити, залишається z2. Отже, кількість синаптичних ваг у CNN у n × m × k/z2 разів менше, ніж SNN для першого прихованого шару. Це називається властивістю розподілу

ваги і зображено на рис. Незважаючи на те, що це пояснення стосувалося першого прихованого шару, воно справедливе для всіх згорткових прихованих шарів. Ця властивість дає CNN дві переваги перед SNN. Перша перевага — це ще менше параметрів для засвоєння машини, а друга — дозволяє CNN шукати певні об’єкти на зображенні, незалежно від того, де вони знаходяться [45].

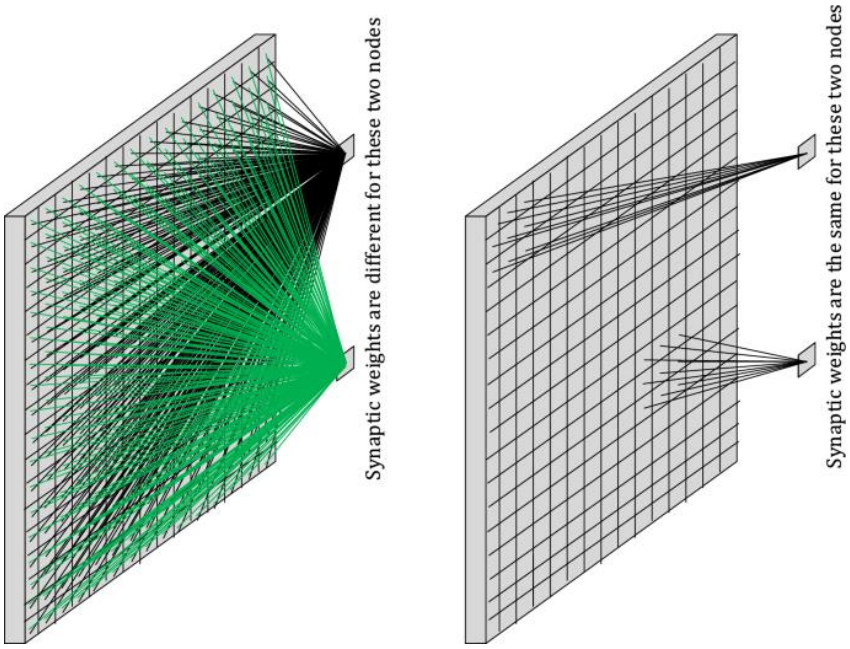


Рис. 2.2. Зіставлення роботи SNN та CNN

2.2. Засоби обробки інформації.

У ході роботи розроблялося модель, ріал-тайм сканування та інтерфейс. Для кожної частини використовувались певні засоби та мові програмування Python.

Для розробки моделі програми використовувався keras з tensorflow.

TensorFlow — це платформа з відкритим кодом для машинного навчання. Він має всеосяжну, гнучку екосистему інструментів, бібліотек і ресурсів спільноти, що дозволяє дослідникам використовувати найсучасніші технології машинного навчання, а розробникам легко створювати й розгортати програми на базі машинного машинного навчання.

Спочатку TensorFlow був розроблений дослідниками та інженерами, які працювали в команді Google Brain в організації Machine Intelligence Research від Google для проведення машинного навчання та дослідження глибоких нейронних мереж. Система досить загальна, щоб її можна було застосувати і в багатьох інших областях.

TensorFlow забезпечує стабільні API Python і C++, а також негарантований зворотно сумісний API для інших мов [https://github.com/tensorflow/tensorflow].

Важливим аспектом є вибір саме TensorFlow, який необхідно обґрунтувати.

Поряд із TensorFlow існує ряд інших бібліотек програмного забезпечення глибокого навчання з відкритим кодом, найпопулярнішими є Theano, Torch і Caffe. Тут досліджується якісні та кількісні відмінності між TensorFlow та кожною з цих альтернатив. Починаю з якісного порівняння «високого рівня» та досліджую, де TensorFlow розходиться або перекривається концептуально чи архітектурно. Потім розгляну кілька джерел кількісних порівнянь.

Якісне порівняння. Порівнюються Theano, Torch і Caffe з TensorFlow відповідно. Малюнок містить огляд найважливіших моментів розмови.

Library	Frontends	Style	Gradients	Distributed Execution
TensorFlow	Python, C++[†]	Declarative	Symbolic	✓[‡]
Theano	Python	Declarative	Symbolic	×
Torch	LuaJIT	Imperative	Explicit	×
Caffe	Protobuf	Imperative	Explicit	×

[†] Very limited API.
[‡] Starting with TensorFlow 0.8, released in April 2016 [16].

Рис. 2.3. Огляд бібліотек

1) Theano: з трьох альтернатив, які ми обговорюємо, Theano, який має інтерфейс Python, найбільше схожий на TensorFlow. Як і TensorFlow, модель програмування Theano є декларативною, а не імперативною, і заснована на обчислювальних графіках. Крім того, Theano використовує

символічну диференціацію, як і TensorFlow. Однак відомо, що Theano має дуже довгий час компіляції графіка, оскільки він перекладає код Python на C++/CUDA [5]. Частково це пов'язано з тим, що Theano застосовує ряд більш просунутих алгоритмів оптимізації графів [5], тоді як TensorFlow наразі виконує лише звичайне видалення підграфів. Крім того, інструменти візуалізації Theano дуже погані в порівнянні з TensorBoard. Поряд із вбудованою функціональністю для виведення простих текстових уявлень графіка або статичних зображень, плагін можна використовувати для створення злегка інтерактивних візуалізацій HTML. Однак він далеко не такий потужний, як TensorBoard. Нарешті, також немає (за готової) підтримки розподілу виконання обчислювального графіка, хоча це є ключовою особливістю TensorFlow. 2) Torch: Однією з принципових відмінностей між Torch і TensorFlow є той факт, що Torch, хоча він має бекенд C/CUDA, використовує Lua як основний інтерфейс. Хоча Lua(JIT) є однією з найшвидших мов сценаріїв і дозволяє швидко створювати прототип і швидке виконання, вона ще не дуже поширена. Це означає, що, хоча навчати та розробляти моделі за допомогою Torch може бути легко, обмежений API та екосистема бібліотек Lua можуть ускладнити промислове розгортання порівняно з бібліотекою на Python, такою як TensorFlow (або Theano). Крім мовного аспекту, модель програмування Torch кардинально відрізняється від TensorFlow. Моделі виражаються в імперативному стилі програмування, а не у вигляді декларативних обчислювальних графіків. Це означає, що програміст повинен, по суті, дбати про порядок виконання операцій. Це також означає, що Torch використовує не символ-символ, а диференціацію символ-число, що вимагає явних прямих і зворотних проходів для обчислення градієнтів. 3) Caffe: Caffe найбільше відрізняється від TensorFlow — різними способами. Хоча існують інтерфейси високого рівня MATLAB і Python до Caffe для створення моделей, його основним інтерфейсом насправді є «мова» Google Protobuf (це більше витончена,

типізована версія JSON), яка дає зовсім інший досвід порівняно з Python. Крім того, основними будівельними блоками в Caffe є не операції, а цілі шари нейронної мережі. У цьому сенсі TensorFlow можна вважати досить низькорівневим у порівнянні. Як і Torch, Caffe не має поняття про обчислювальні графіки чи символи, тому обчислює похідні за допомогою підходу від символу до числа. Caffe особливо добре підходить для розробки згорткових нейронних мереж і завдань розпізнавання зображень, однак він не досягає багатьох інших найсучасніших категорій, які добре підтримуються TensorFlow. Наприклад, Caffe за задумом не підтримує циклічні архітектури, які становлять основу RNN, LSTM та інших моделей. У Caffe немає підтримки розподіленого виконання.

Кількісне порівняння. Тепер розгляну три джерела кількісних порівнянь між TensorFlow та іншими бібліотеками глибокого навчання, надавши короткий підсумок найважливіших результатів кожної роботи. Крім того, коротко обозначу загальну тенденцію цих контрольних показників. У першій роботі [20], автором якої був науково-технічний центр Bosch, порівнюється продуктивність TensorFlow, Torch, Theano і Caffe (серед інших) щодо різних архітектур нейронних мереж. Їх налаштування включає в себе Ubuntu 18.04, що працює на процесорі Intel Xeon E5-1650 v2 на 3,50 ГГц і графічному процесорі NVIDIA GeForce GTX Titan X/PCIe/SSE2. Одним з контрольних показників вважаю, що заслуговують на увагу, тести відносної продуктивності кожної бібліотеки на дещо зміненому відтворенні моделі LeNet CNN [21]. Більш конкретно, автори вимірюють час прямого поширення, який вони вважають релевантним для розгортання моделі, і час зворотного поширення, важливий для навчання моделі. Уривок їхніх результатів відтворено у рис., де показано їхні результати на (а) ЦП з 12 потоками та (б) ГП.

Library	Forward (ms)	Backward (ms)
TensorFlow	16.4	50.1
Torch	**4.6**	**16.5**
Caffe	33.7	66.4
Theano	78.7	204.3

(a) CPU (12 threads)

Library	Forward (ms)	Backward (ms)
TensorFlow	4.5	14.6
Torch	**0.5**	1.7
Caffe	0.8	1.9
Theano	**0.5**	**1.4**

(b) GPU

Рис. 2.4. Огляд бібліотек

Цікаво, що для (a) TensorFlow займає друге місце після Torch як за прямим, так і за зворотним показником, тоді як у (b) продуктивність TensorFlow значно падає, поміщаючи його на останнє місце в обох категоріях. Автори [20] відзначають, що однією з причин цього може бути те, що вони використовували бібліотеку NVIDIA cuDNN v2 для реалізації GPU за допомогою TensorFlow, а для інших — cuDNN v3. Вони стверджують, що на момент їх написання це була рекомендована конфігурація для TensorFlow [27]. Другим джерелом у колекції є репозиторій convnetbenchmarks на GitHub від Соміта Чінтала [22], інженера-дослідника штучного інтелекту у Facebook. Чінтала надає широкий набір тестів для різноманітних моделей згорткових мереж і включає багато бібліотек, включаючи TensorFlow, Torch і Caffe у своїх вимірюваннях. Theano присутній не у всіх тестах, тому я не буду переглядати його продуктивність у цьому наборі тестів. Апаратна конфігурація автора — це 6-ядерний процесор Intel Core i7-5930K @ 3,50 ГГц і графічний чіп NVIDIA Titan X, що працює на Ubuntu 18.04. Серед іншого, Chintala дає час поширення в прямому і зворотному напрямку для TensorFlow, Torch і Caffe для моделі AlexNet CNN [23]. У цих контрольних показниках TensorFlow займає друге місце в обох показниках після Torch, а Caffe відносно значно відстає. Відповідні результати ми відтворюємо в рис.

Library	Forward (ms)	Backward (ms)
TensorFlow	26	55
Torch	**25**	**46**
Caffe	121	203
Theano	–	–

Рис. 2.5. Огляд бібліотек

Нарешті, розглянемо результати роботи [5], опубліковану командою розробників Theano. Окрім набору тестів для чотирьох популярних моделей CNN, включаючи вищезгадану архітектуру AlexNet, робота також містить результати для мережі LSTM працює на базі даних Penn Treebank [24]. Їх контрольні показники вимірюють слова, оброблені в секунду для невеликої моделі, що складається з одного прихованого шару в 200 одиниць з довжиною послідовності 20, і великої моделі з двома прихованими шарами по 650 одиниць і довжиною послідовності 50. У [5] також середній шар - розмірна модель тестується, що ми ігноруємо для нашого огляду. Автори заявляють про апаратну конфігурацію, що складається з NVIDIA Digits DevBox з 4 графічними процесорами Titan X і процесором Intel Core i7-5930K. Більше того, вони використовували cuDNN v4 для всіх бібліотек, включених в їхні тести, а саме TensorFlow, Torch і Theano. Результати для Caffe не надаються. У їхніх тестах TensorFlow працює найкраще серед усіх трьох для маленької моделі, за ним слідують Theano, а потім Torch. Для великої моделі TensorFlow посідає друге місце після Theano, а Torch залишається на останньому місці. На рис. наведено ці результати, взяті з [46].

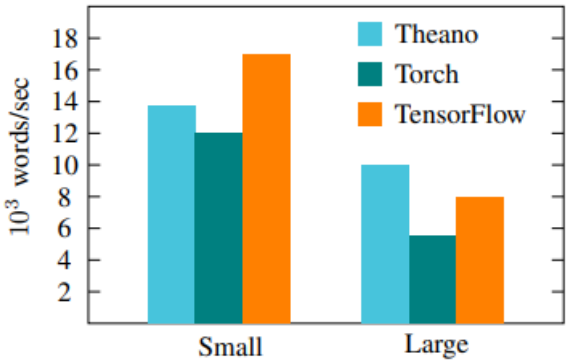


Рис. 2.6. Огляд продуктивності бібліотек

Перейдемо до більш високорівневих бібліотек. Keras — це API глибокого навчання, написаний на Python, який працює поверх платформи машинного навчання TensorFlow. Він був розроблений з упором на можливість швидкого експериментування. Вміння якнайшвидше переходити від ідеї до результату є ключем до хорошого дослідження.

Keras - це:

• простий, але не спрощений. Keras зменшує когнітивне навантаження розробника, щоб ви могли зосередитися на тих частинах проблеми, які дійсно важливі.

• гнучкість – Keras використовує принцип прогресивного розкриття складності: прості робочі процеси мають бути швидкими та легкими, тоді як довільно розширені робочі процеси мають бути можливими за допомогою чіткого шляху, який спирається на те, що ви вже навчилися.

• потужний — Keras забезпечує потужну продуктивність і масштабованість: його використовують організації та компанії, зокрема NASA, YouTube або Waymo.

Зараз поговоримо про шари моделі:

- Dense - просто ваш звичайний щільно пов'язаний шар NN;

- Input - шар, який буде використовуватися як точка входу в мережу (графік шарів);

- Dropou - застосовує Dropout до входу;

- GlobalAveragePooling2D - глобальна середня операція об'єднання просторових даних;

- Flatte - вирівнює введення. Не впливає на розмір партії;

- Conv2D - шар 2D згортки (наприклад, просторова згортка над зображеннями);

- BatchNormalization - шар, який нормалізує свої вхідні дані;

- Activation - застосовує функцію активації до виходу;

- MaxPooling2D - максимальна операція об'єднання для 2D просторових даних.

Matplotlib — це повна бібліотека для створення статичних, анімованих та інтерактивних візуалізацій на Python. Matplotlib робить легкі речі легкими, а важкі можливими.

- Створення якісних графіків;

- можливість зробити інтерактивні фігури, які можна масштабувати, панорамувати, оновлювати

- налаштування візуального стилю та макету.;

- експорт у багато форматів файлів;

- вбудовуваний в JupyterLab і графічні інтерфейси користувача;

- використання багатого набіру сторонніх пакетів, створених на Matplotlib.

Numpy – бібліотека для здійснення обчислень.

Pandas – бібліотека для роботи з даними.

Seaborn – бібліотека для візуалізації даних.

cv2 — неофіційні попередньо вбудовані пакети OpenCV для Python лише для ЦП.

2.3. Цінність розробки проекту з точки зору психології.

Виявлення особливостей характеру через обробку фотографій не є новим напрямком. Наприклад, хотілося б описати деякі здобутки в цій сфері

і показати підхід, який використовується в даній роботі для розпізнавання особливостей.

Все більше досліджень пов’язують зображення обличчя з особистістю. Встановлено, що люди здатні сприймати певні риси особистості на обличчях один одного з певним ступенем точності [1–4]. На додаток до емоційних виразів та інших невербальних форм поведінки, які передають інформацію про психологічні процеси через обличчя, дослідження виявили, що дійсні висновки про особистісні характеристики можна зробити навіть на основі статичних зображень обличчя з нейтральним виразом [5–7]. Ці висновки свідчать про те, що люди можуть використовувати сигнали з обличь один одного, щоб коригувати спосіб спілкування залежно від емоційних реакцій та уявлення про особистість співрозмовника. Такі сигнали мають бути досить інформативними та достатньо повторюваними, щоб одержувачі могли скористатися перевагами інформації, що передається [8]. Дослідження, присвячені об’єктивним характеристикам людських обличь, виявили певні асоціації між морфологією обличчя та рисами особистості.

Наприклад, симетрія обличчя передбачає екстраверсію [9]. Іншим широко досліджуваним показником є відношення ширини обличчя до висоти (fWHR), яке було пов’язано з різними рисами, такими як прагнення досягти [10], обман [11], домінування [12], агресивність [13–16] та ризикування [17]. fWHR можна виявити з високою надійністю незалежно від волосся на обличчі. Точність суджень на основі fWHR свідчить про те, що система сприйняття людини, можливо, стала чутливою до статичних рис обличчя, таких як відносна ширина обличчя [18]. Є кілька теоретичних причин очікувати зв’язку між зображеннями обличчя та особистістю. По-перше, генетичне походження впливає як на обличчя, так і на особистість. Генетичні кореляти черепно-лицевих характеристик були виявлені як у клінічних контекстах [19,20], так і в доклінічних популяціях [21]. Окрім

формування обличчя, гени також відіграють роль у розвитку різних рис особистості, таких як ризикована поведінка [22–24], а внесок генів у деякі риси перевищує внесок факторів навколишнього середовища [25]. Для ознак Великої п’ятірки коефіцієнти спадковості, що відображають частку дисперсії, яка може бути пов’язана з генетичними факторами, зазвичай лежать в діапазоні 0,30–0,6026,27. З еволюційної точки зору, можна очікувати, що ці асоціації виникнуть за допомогою статевого відбору. Недавні дослідження стверджують, що деякі статичні риси обличчя, такі як супраорбітальна область, могли еволюціонувати як засіб соціальної комунікації [28] і що привабливість обличчя, що сигналізує про цінні характеристики особистості, пов’язана з успіхом спарювання29. По-друге, є деякі докази того, що пре- і постнатальні гормони впливають як на форму обличчя, так і на особистість. Наприклад, обличчя є видимим індикатором рівня статевих гормонів, таких як тестостерон та естроген, які впливають на формування кісток черепа та fWHR [30–32]. Враховуючи, що пренатальний і постнатальний рівень статевих гормонів впливає на поведінку, риси обличчя можуть корелювати з гормонально обумовленими характеристиками особистості, такими як агресивність [33], конкурентоспроможність і домінування, принаймні для чоловіків [34,35]. Крім генів, зв’язок рис обличчя з поведінковими тенденціями також можна пояснити андрогенами та потенційно іншими гормонами, які впливають як на обличчя, так і на поведінку. По-третє, сприйняття рис свого обличчя собою та іншими впливає на подальшу поведінку та особистість [36]. Подібно до того, як уявлення про «розумність» індивіда може призвести до вищого рівня освіти [37], упередження, пов’язані з формою обличчя, можуть призвести до розвитку дезадаптивних характеристик особистості (тобто «комплекс Квазімодо» [38]). Асоціації між зовнішнім виглядом і особистістю протягом тривалості життя були досліджені в лонгітюдних

обсерваційних дослідженнях, надавши докази ефектів типу «самоздійснюване пророцтво» та «саморуйнівного пророцтва» [39].

По-четверте, і останнє, деякі риси особистості пов’язані зі звичними моделями емоційно-експресивної поведінки. Звичні емоційні вирази можуть формувати статичні риси обличчя, що призводить до утворення зморшок та/або розвитку мімічних м’язів.

Існуючі дослідження виявили зв’язок між об’єктивними ознаками зображення обличчя та загальними рисами особистості на основі моделі особистості з п’яти факторів або моделі великої п’ятірки (BF) [40]. Однак швидкий погляд на розміри ефектів, знайдених у цих дослідженнях (зведених у таблиці 1), виявляє багато суперечок. Результати видаються суперечливими в різних дослідженнях і важко відтворюваними [41]. Такі невідповідності можуть бути результатом використання невеликих зразків обличь стимулів, а також величезних відмінностей у методологіях. Більш сильні розміри ефекту зазвичай виявляють у дослідженнях із використанням композиційних зображень обличчя, отриманих від груп людей з високими та низькими балами за кожним з вимірів Великої п’ятірки [6–8]. Отож, завдання ідентифікації ознак за допомогою штучних зображень, що складаються з контрастних пар з усіма іншими індивідуальними ознаками, виключеними або незмінними, видається відносно легкою. Це відрізняється від реалістичних ситуацій, коли обличчя людей відображають повний спектр безперервних характеристик особистості, закладених у різноманітні індивідуальні риси обличчя.

Також, наведу приклад точності роботи, що займалась дослвдженням між обличчям та характеристиками з «великої п’ятірки».

У статті використовували дані з тестового набору даних, що містить прогнозовані бали для 3137 зображень, пов’язаних з 1245 особами. Щоб визначити, чи була дисперсія прогнозованих оцінок пов’язана з відмінностями між зображеннями чи між індивідами, розрахували

коефіцієнти внутрішньокласової кореляції (ICC), представлені на малюнку. Частка дисперсії між індивідами в прогнозованих балах коливалася від 79 до 88% для різних ознак, що вказує на загальну узгодженість прогнозованих балів для різних фотографій однієї особи. Вивели індивідуальні бали, які використовувалися в усіх наступних аналізах, як прості середні значення прогнозованих балів для всіх зображень, наданих кожним учасником.

Trait	Gender	ICC	r	ρ	RMSE	MAE
Agreeableness	Men	0.829 [0.802; 0.852]	0.214 [0.129; 0.295]	0.230	1.253 (1.404)	0.964 (1.100)
	Women	0.811 [0.789; 0.832]	0.238 [0.168; 0.304]	0.254	1.234 (1.378)	0.981 (1.090)
Conscientiousness	Men	0.853 [0.830; 0.873]	0.360 [0.281; 0.433]	0.386	1.130 (1.419)	0.889 (1.130)
	Women	0.821 [0.800; 0.841]	0.335 [0.270;0.398]	0.358	1.152 (1.424)	0.897 (1.140)
Extraversion	Men	0.827 [0.800; 0.851]	0.187 [0.102;0.270]	0.202	1.274 (1.338)	1.019 (1.070)
	Women	0.785 [0.760; 0.809]	0.266 [0.198;0.332]	0.288	1.211 (1.407)	0.945 (1.100)
Neuroticism	Men	0.803 [0.773; 0.830]	0.210 [0.125;0.292]	0.220	1.255 (1.408)	0.995 (1.100)
	Women	0.849 [0.830; 0.866]	0.284 [0.216;0.349]	0.295	1.196 (1.453)	0.951 (1.170)
Openness	Men	0.855 [0.832; 0.875]	0.189 [0.104;0.272]	0.224	1.272 (1.382)	0.986 (1.100)
	Women	0.876 [0.860; 0.890]	0.137 [0.067;0.207]	0.161	1.313 (1.443)	1.036 (1.130)

Рис. 2.7. Огляд результатів [2]

Коефіцієнти кореляції між результатами тесту самозвіту та оцінками, передбаченими ANN, становили від 0,14 до 0,36. Асоціації були найсильнішими за сумлінність і найслабшими за відкритість. Екстраверсія та невротизм були значно краще прогнозовані для жінок, ніж для чоловіків (на основі z-тесту). Також порівняли точність прогнозу для кожної статі за допомогою тесту Стейгера для залежних коефіцієнтів кореляції вибірки. Для чоловіків сумлінність передбачалася точніше, ніж інші чотири ознаки (різниці між останніми не були статистично значущими). Для жінок сумлінність передбачалася точніше, а відкритість — менш точно в порівнянні з трьома іншими ознаками. Середня абсолютна похибка (MAE) прогнозу коливалася від 0,89 до 1,04 стандартних відхилень. не знайшли жодних зв'язків між кількістю фотографій і помилкою прогнозу. Тобто точність дослідження була високою [2].

2.4. Висновки після другого розділу

В розділі було детально описано методи та засоби обробки інформації для дослідження. Обговорено TensorFlow, нову бібліотеку глибокого навчання з відкритим кодом, засновану на обчислювальних графіках. Його здатність виконувати швидкі автоматичні обчислення градієнта, притаманна йому підтримка розподілених обчислень і спеціалізованого обладнання, а також потужні інструменти візуалізації роблять його дуже бажаним доповненням до області машинного навчання. Його низькорівневий інтерфейс програмування дає дрібнозернистий контроль побудови нейронної мережі, тоді як бібліотеки абстракції, такі як TFLearn, дозволяють швидко створювати прототип за допомогою TensorFlow. У контексті інших інструментів глибокого навчання, таких як Theano або Torch, TensorFlow додає нові функції та покращує інші. Його продуктивність була нижчою, ніж спочатку, але покращується з новими випусками бібліотеки. TensorFlow здобув велику популярність і сильну підтримку в спільноті з відкритим кодом завдяки багатьом внескам третіх сторін, що вже робить крок Google розумним рішенням.

Також було описано підхід визначення певних рис характеру з точки зору психології. Показано, що існує багато доказів того, що морфологічні та соціальні ознаки на обличчі людини дають сигнали людської особистості та поведінки. Попередні дослідження виявили зв’язок між особливостями штучних композиційних зображень обличчя та атрибуцією рис особистості експертами з людей. Аналіз переконливо підтверджує можливість прогнозування багатовимірних профілів особистості на основі статичних зображень обличчя за допомогою МНС, навчених на великих наборах даних. Майбутні дослідження могли б досліджувати відносний внесок морфологічних особливостей обличчя та інших характеристик зображень обличчя в прогнозування особистості.

РОЗДІЛ 3. ПОБУДОВА МОДЕЛІ ПРОГНОЗУВАННЯ СКОЄНОГО ЗЛОЧИНУ ПО ЗОВНІШНОСТІ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

3.1.Візуалізація вхідних даних проекту обробки інформації.

Дані були узяті з таких ресурсів, як:

1) FBI ресурси

1.1) Terrorism – FBI [47];

1.2) Wanted Bank Robbers – [48];

1.3) Figutives – FBI [49];

2) Interpol Red Notice [50].

Зображення всі у форматі png. Зображення змішаної раси, змішаної статі та нейтрального виразу обличчя і містять як спереду, так і збоку (профіль). Оскільки ми зосереджуємось на фронтальних знімках обличчя, нам потрібно виключити перегляди профілю. Каскадний класифікатор виявляє зображення, що містять фронтальні види обличчя, а також виявляє прямокутну область, що містить обличчя. Зображення передаються в попередньо підготовлену версію цього класифікатора, доступну в бібліотеці OPenCV в Python, щоб зберегти лише зображення, які містять фронтальні види граней, а потім обрізати прямокутну область, що містить обличчя. Обрізання прямокутника обличчя від решти зображення запобігає впливу на класифікатор периферійних або фонових ефектів, що оточують обличчя. Рівень помилкових позитивних результатів (зображення без фронтальних облич, неправильно класифіковані як зображення фронтальних облич) каскадного класифікатора становив 1,9%, які були видалені вручну. Оскільки нейронні мережі отримують вхідні дані однакового розміру, розмір усіх зображень змінюється до 48×48 за допомогою білінійної інтерполяції. Цей розмір вибрано з урахуванням платформи, на якій розробляється програма.

Використовується по 225 фотографій кожного типу (законопорядні, терористи, грошові крадії та вбивці) для тренування НМ, та по 25 для тестування. Тобто 90% на 10%.

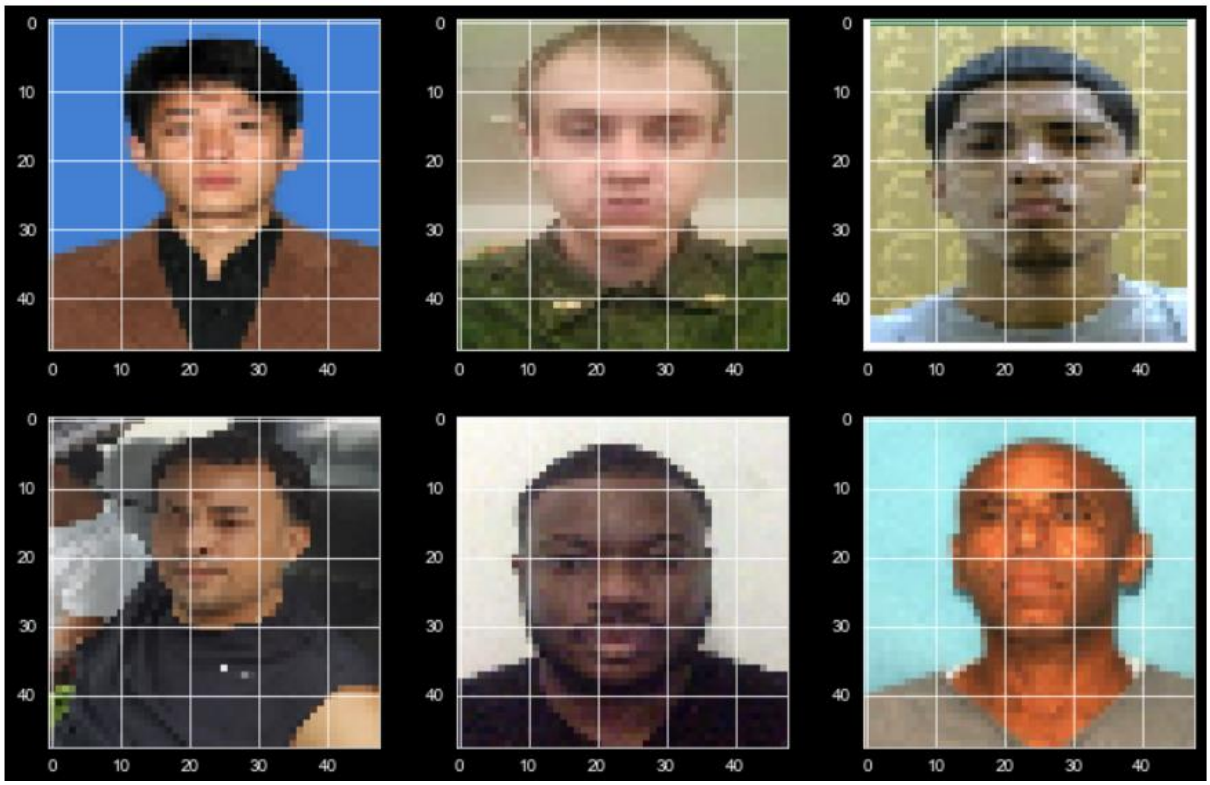


Рис. 3.1. Візуалізація датасету

3.2.Представлення поетапної обробки даних засобами обробки інформації.

Зараз буде описано які етапи обробки інформації було пройдено для отримання результатів. Архітектура CNN включає кілька будівельних блоків, таких як шари згортки, шари об’єднання та повністю підключені шари. Типова архітектура складається з повторень стека з кількох шарів згортки та шару об’єднання, за яким слідують один або кілька повністю пов’язаних шарів. Крок, на якому вхідні дані перетворюються у вихідні через ці шари, називається прямим поширенням. Описані в цьому розділі операції згортки та об’єднання призначені для 2D-CNN.

Шар згортки. Рівень згортки є основним компонентом архітектури CNN, який виконує вилучення ознак, яке зазвичай складається з комбінації лінійних і нелінійних операцій, тобто операції згортки та функції активації.

Згортка. Згортка — це спеціалізований тип лінійної операції, що використовується для вилучення ознак, де невеликий масив чисел, який називається ядром, застосовується до вхідних даних, який є масивом чисел, який називається тензором. Поелементний добуток між кожним елементом ядра та вхідним тензором обчислюється в кожному місці тензора і підсумовується, щоб отримати вихідне значення у відповідній позиції вихідного тензора, яке називається картою ознак (рис. 3a–c). . Ця процедура повторюється із застосуванням кількох ядер для формування довільної кількості карт ознак, які представляють різні характеристики вхідних тензорів; Таким чином, різні ядра можна розглядати як екстрактори різних ознак. Двома ключовими гіперпараметрами, які визначають операцію згортки, є розмір і кількість ядер. Перший зазвичай становить 3×3, але іноді 5×5 або 7×7. Останній є довільним і визначає глибину вихідних карт об’єктів.

Операція згортки, описана вище, не дозволяє центру кожного ядра перекривати крайній елемент вхідного тензора і зменшує висоту та ширину вихідної карти об’єктів порівняно з вхідним тензором. Заповнення, як правило, нульове заповнення, є методом вирішення цієї проблеми, коли рядки та стовпці нулів додаються з кожної сторони вхідного тензора, щоб умістити центр ядра на крайньому зовнішньому елементі та зберегти ту саму площину. розмір через операцію згортки. Сучасні архітектури CNN зазвичай використовують нульове заповнення, щоб зберегти розміри в площині, щоб застосувати більше шарів. Без нульового заповнення кожна наступна карта об’єктів буде зменшуватися після операції згортки.

Відстань між двома послідовними положеннями ядра називається кроком, який також визначає операцію згортки. Загальний вибір кроку – 1;

однак крок, більший за 1, іноді використовується для досягнення зниження дискретизації карт ознак. Альтернативною технікою виконання зниження дискретизації є операція об'єднання, як описано нижче.

Ключовою особливістю операції згортки є розподіл ваги: ядра використовуються спільно для всіх позицій зображення. Розподіл ваги створює такі характеристики операцій згортки: (1) дозволяючи шаблонам локальних ознак, витягнутим за допомогою трансляції ядра b, бути інваріантними, оскільки ядра переміщуються по всіх позиціях зображення та виявляють вивчені локальні шаблони, (2) вивчення просторової ієрархії шаблонів ознак шляхом зменшення дискретизації в у поєднанні з операцією об’єднання, що призводить до захоплення все більшого поля зору та (3) підвищення ефективності моделі за рахунок зменшення кількості параметрів для вивчення в порівнянні з повністю підключеними нейронними мережами.

Як описано пізніше, процес навчання моделі CNN щодо шару згортки полягає у визначенні ядер, які найкраще працюють для даного завдання на основі заданого набору навчальних даних. Ядра є єдиними параметрами, які автоматично вивчаються під час процесу навчання в шарі згортки; з іншого боку, розмір ядер, кількість ядер, відступ і крок є гіперпараметрами, які необхідно встановити перед початком процесу навчання.

Нелінійна функція активації. Вихідні дані лінійної операції, наприклад згортки, потім передаються через нелінійну функцію активації. Хоча гладкі нелінійні функції, такі як сигмовидна або гіперболічна тангенс (tanh), використовувалися раніше, оскільки вони є математичним уявленням поведінки біологічного нейрона, найпоширенішою нелінійною функцією активації, яка використовується зараз, є випрямлена лінійна одиниця (ReLU), яка просто обчислює функція: $f(x) = \max(0, x)$ [35, 36, 37, 38, 39].

Об’єднуючий шар. Рівень об’єднання забезпечує типову операцію зниження дискретизації, яка зменшує розмірність у площині карт ознак, щоб ввести інваріантність трансляції до невеликих зсувів і спотворень, а також зменшити кількість наступних параметрів, які можна вивчати. Слід зазначити, що в жодному з шарів об’єднання немає параметрів, які можна вивчати, тоді як розмір фільтра, крок і заповнення є гіперпараметрами в операціях об’єднання, подібними до операцій згортки.

.Максимальний пул. Найпопулярнішою формою операції об’єднання є максимальний пул, який витягує латки з вхідних карт об’єктів, виводить максимальне значення в кожному патчі та відкидає всі інші значення. На практиці зазвичай використовується максимальне об’єднання з фільтром розміром 2 × 2 з кроком 2. Це зменшує розмірність у площині карт об’єктів у 2 рази. На відміну від висоти та ширини, розмір глибини карт об’єктів залишається незмінним.

Глобальне середнє об’єднання. Ще одна операція об’єднання, на яку варто звернути увагу, — це глобальне середнє об’єднання [40]. Глобальне середнє об’єднання виконує екстремальний тип зниження дискретизації, коли карта об’єктів розміром висота × ширина зменшується до масиву 1 × 1, просто взявши середнє значення всіх елементів у кожній карті об’єктів, тоді як глибина карт об’єктів дорівнює зберігається. Ця операція зазвичай застосовується лише один раз перед повністю з’єднаними шарами. Переваги застосування глобального середнього пулу полягають у наступному: (1) зменшує кількість параметрів, які можна вивчати, і (2) дає змогу CNN приймати вхідні дані змінного розміру.

Повністю пов'язаний шар. Вихідні карти об’єктів остаточного шару згортки або об’єднання зазвичай згладжуються, тобто перетворюються в одновимірний (1D) масив чисел (або вектор) і з’єднуються з одним або кількома повністю пов’язаними шарами, також відомими як щільні шари, в якому кожен вхід пов’язаний з кожним виходом за допомогою ваги, яку

можна вивчати. Після того, як об’єкти, виділені шарами згортки та зменшені шарами об’єднання, створені, вони відображаються підмножиною повністю пов’язаних шарів на кінцеві вихідні дані мережі, наприклад, ймовірності для кожного класу в завданнях класифікації. Останній повністю підключений шар зазвичай має таку ж кількість вихідних вузлів, як і кількість класів. За кожним повністю підключеним шаром слідує нелінійна функція, така як ReLU, як описано вище.

Функція активації останнього шару. Функція активації, застосована до останнього повністю підключеного шару, зазвичай відрізняється від інших. Відповідно до кожного завдання необхідно вибрати відповідну функцію активації. Функція активації, застосована до завдання мультикласової класифікації, є функцією softmax, яка нормалізує вихідні реальні значення з останнього повністю підключеного шару до ймовірностей цільового класу, де кожне значення знаходиться в діапазоні від 0 до 1, а сума всіх значень дорівнює 1. Типовий вибір останнього рівня функція активації для різних типів завдань зведена в таблиці 2 [24].

3.3.Візуалізація результату аналізу.

Навчання мережі – це процес пошуку ядер у шарах згортки та ваг у повністю зв’язаних шарах, що мінімізує відмінності між вихідними передбаченнями та заданими основними мітками істинності в наборі навчальних даних. Алгоритм зворотного поширення — це метод, який зазвичай використовується для навчання нейронних мереж, де важливу роль відіграють функція втрат і алгоритм оптимізації градієнтного спуску. Продуктивність моделі для певних ядер і ваг розраховується функцією втрат шляхом прямого поширення на наборі даних для навчання, а параметри, які можна вивчати, а саме ядра та ваги, оновлюються відповідно до значення втрат за допомогою алгоритму оптимізації, який називається зворотним поширенням і градієнтним спуском, серед інших.

Функція втрати. Функція втрат, яку також називають функцією вартості, вимірює сумісність між вихідними передбаченнями мережі через пряме поширення та заданими наземними мітками істинності. Функцією втрат для багатокласової класифікації є перехресна ентропія, тоді як середня квадратична помилка зазвичай застосовується до регресії до безперервних значень. Тип функції втрат є одним із гіперпараметрів і потребує визначення відповідно до поставлених завдань.

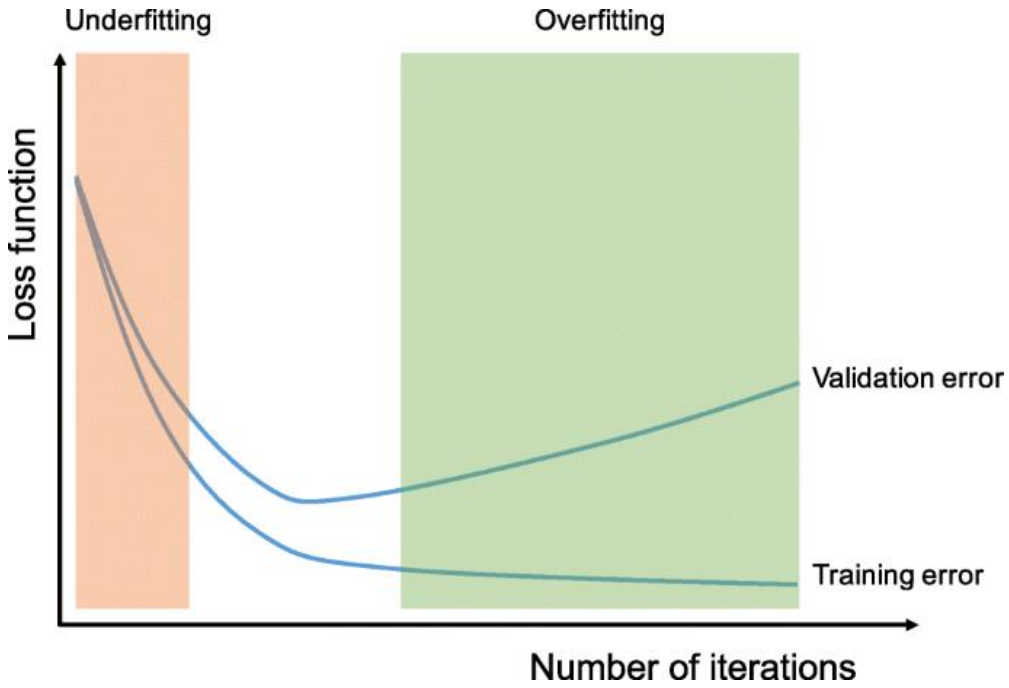


Рис. 3.2. Візуалізація функції втрат

Градієнтний спуск. Градієнтний спуск використовується як алгоритм оптимізації, який ітеративно оновлює доступні для навчання параметри, тобто ядра та ваги, мережі, щоб мінімізувати втрати. Градієнт функції втрат дає нам напрямок, у якому функція має найбільшу швидкість зростання, і кожен параметр, який можна вивчати, оновлюється в негативному напрямку градієнта з довільним розміром кроку, визначеним на основі гіперпараметра, який називається швидкістю навчання (рис. 3.3). Математично градієнт є частковою похідною від втрати по відношенню до

кожного параметра, що вивчається, і одноразове оновлення параметра формулюється таким чином:

$$w := w - \alpha * \frac{\partial L}{\partial w}$$

де w означає кожен параметр, який можна вивчати, α означає швидкість навчання, а L означає функцію втрат. Слід зазначити, що на практиці швидкість навчання є одним із найважливіших гіперпараметрів, які необхідно встановити перед початком навчання. На практиці, з таких причин, як обмеження пам'яті, градієнти функції втрат щодо параметрів обчислюються за допомогою підмножини навчального набору даних, що називається міні-пакетом, і застосовуються до оновлення параметрів. Цей метод називається градієнтним спуском міні-партії, який також часто називають стохастичним градієнтним спуском (SGD), а розмір міні-партії також є гіперпараметром. Крім того, було запропоновано і широко використовується багато вдосконалень алгоритму градієнтного спуску, таких як SGD з імпульсом, RMSprop і Adam [25, 26, 27], де остання використовується у роботі.

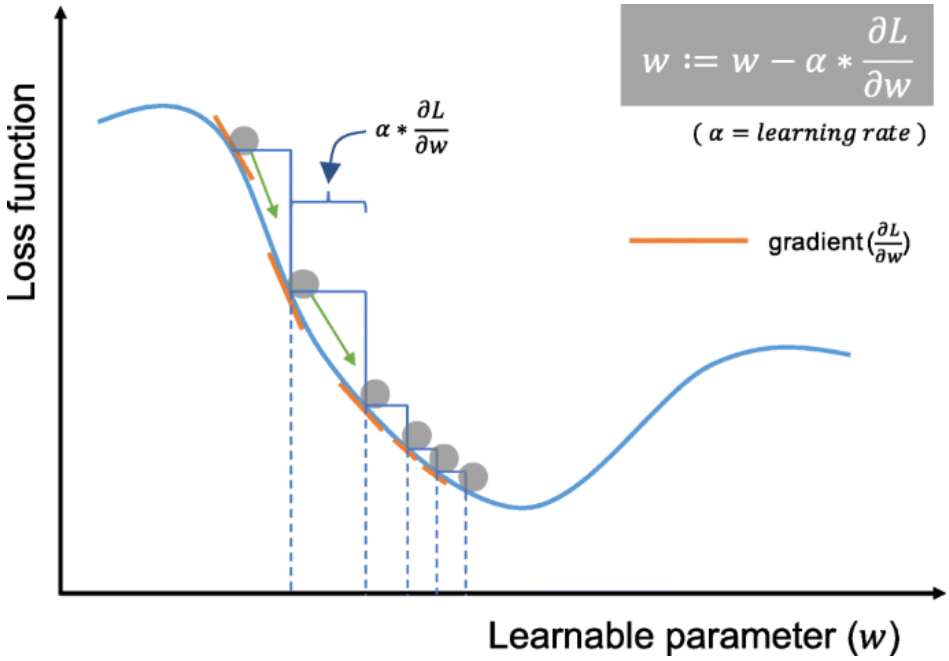


Рис. 3.3. Візуалізація градієнту

На 14-ій епохі навчвння точність досягла 73%, що є найкращим результатом для даного набору даних, що показано на рис 3.4.

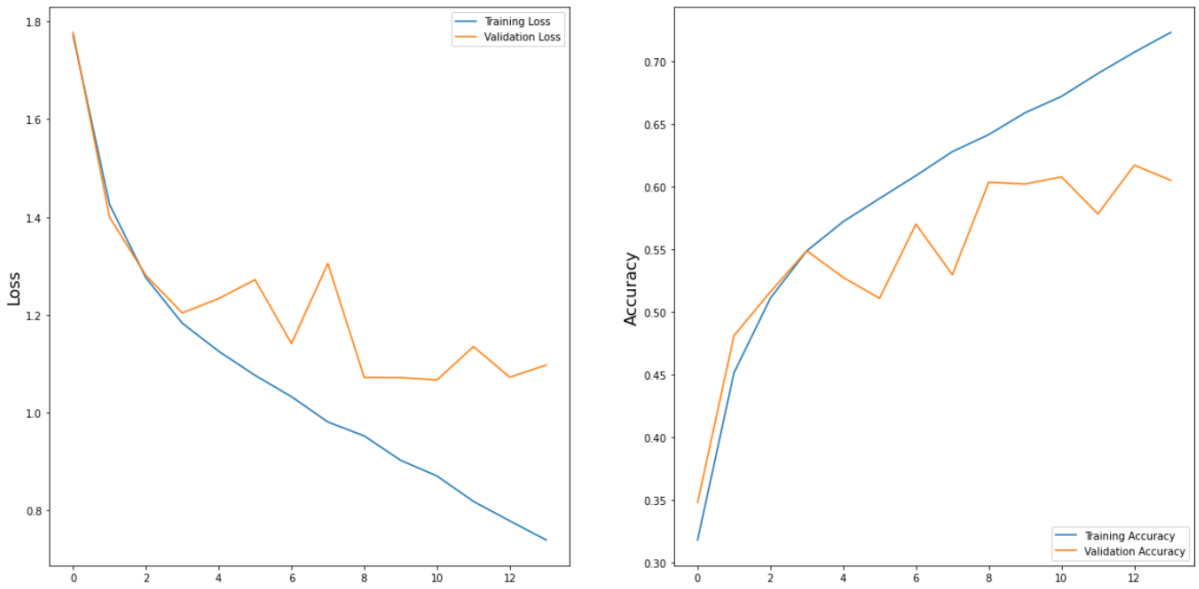


Рис. 3.4. Візуалізація результату

Обґрунтую малу кількість епох навчання. По-перше, впливає обсяг датасету, шо не є великим. По-друге, впливає перенавчання. Але чому це має значення? Напевно, можна б просто збільшити кількість прихованих шарів у нашій мережі і, можливо, збільшити кількість нейронів у них? Проста відповідь на це питання – ні. Це зумовлено двома причинами, однією з яких є проста проблема відсутності необмеженої обчислювальної потужності та часу для навчання цих величезних ІНС. Друга причина — припинення або зменшення наслідків переобладнання. Переобладнання – це в основному, коли мережа не може ефективно навчатися через ряд причин. Це важлива концепція більшості, якщо не всіх алгоритмів машинного навчання, і важливо вжити всіх запобіжних заходів, щоб зменшити його наслідки. Якщо наші моделі будуть демонструвати ознаки переобладнання, ми можемо побачити знижену здатність визначити узагальнені функції не тільки для нашого набору даних для навчання, але також для наших тестів і

наборів прогнозів. Це головна причина зниження складності наших ANN. Чим менше параметрів потрібно для навчання, тим менша ймовірність того, що мережа переобладнається - і, звичайно, покращить прогнозну продуктивність моделі [23].

3.4.Висновки після третього розділу.

У ході розділу було описано та візуалізовано вхідні дані, описано природу їх походження.

Далі була розписана поетапна обробка даних. Згорткова нейронна мережа (CNN), клас штучних нейронних мереж, який став домінуючим у різних задачах комп'ютерного зору, привертає інтерес у різних областях, включаючи радіологію. CNN розроблено для автоматичного та адаптивного вивчення просторової ієрархії функцій за допомогою зворотного поширення за допомогою кількох будівельних блоків, таких як шари згортки, шари об'єднання та повністю пов'язані шари.

Також було візуалізовано такі результати, як втрати та точність. Обґрунтована оптимальна кількість епох навчання.

РОЗДІЛ 4. РОЗРОБКА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОГНОЗУВАННЯ СКОЄНОГО ЗЛОЧИНУ ПО ЗОВНІШНОСТІ ТА РЕКОМЕНДАЦІЇ ЩОДО ЙОГО ВИКОРИСТАННЯ

4.1 Реалізації інформаційного забезпечення прогнозування

Задля зручного застосування технологією біло розроблено інтерфейс програми, який дає змогу тренувати модель та використовувати її. Звісно, це лише візуальне оформлення для зручності використання, та на масштабному півні програма буде мати інший вигляд, як мінімум підключена до камер спостерігання, а не до веб-камери комп'ютера.

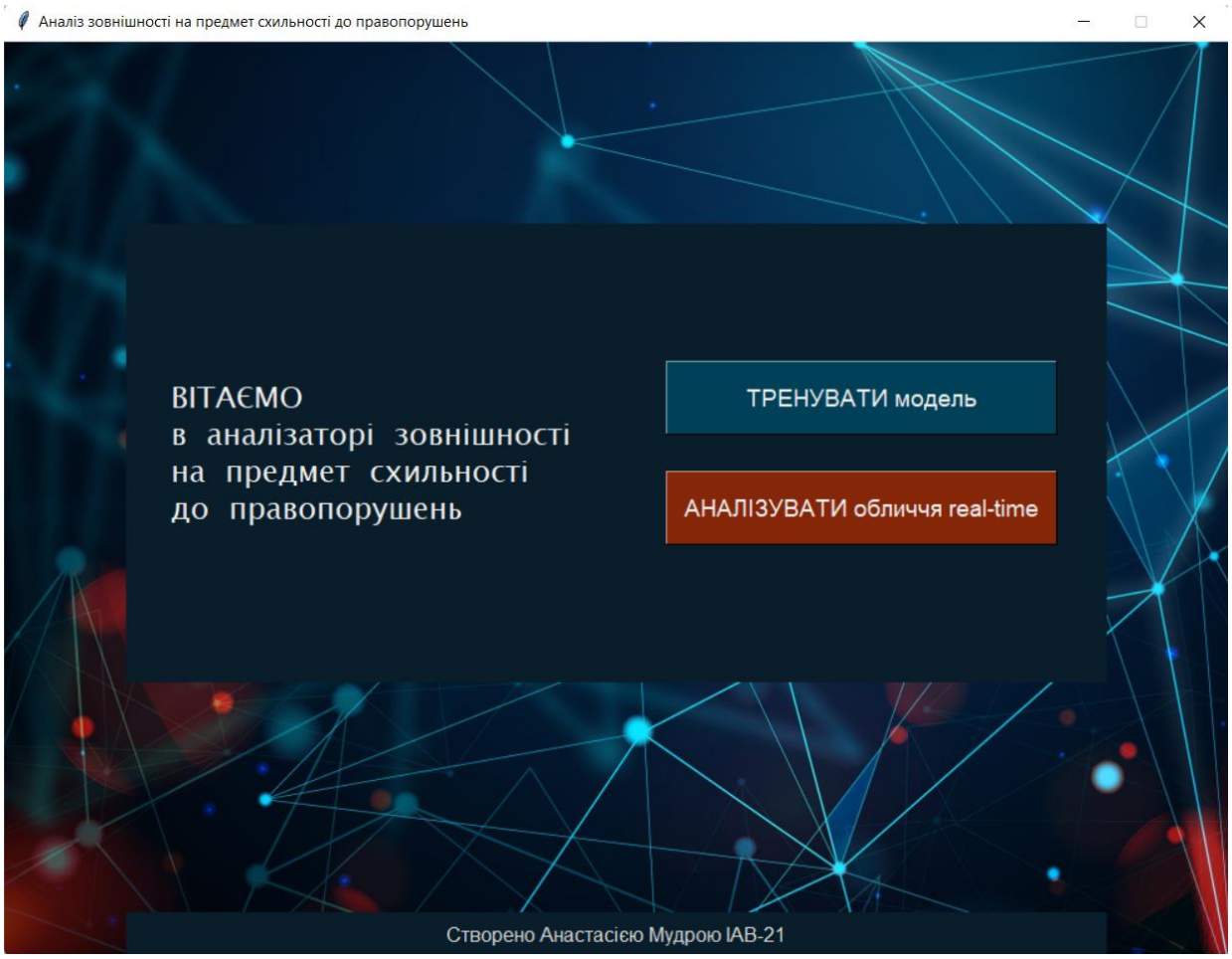


Рис. 4.1. Головний екран

Програма складається з головного екрану, кнопки, що запускає навчання моделі та кнопки, щр запускає сам аналізатор.

Предемонстрю декілька кейсів використання програми аналізатора в режимі real-time.

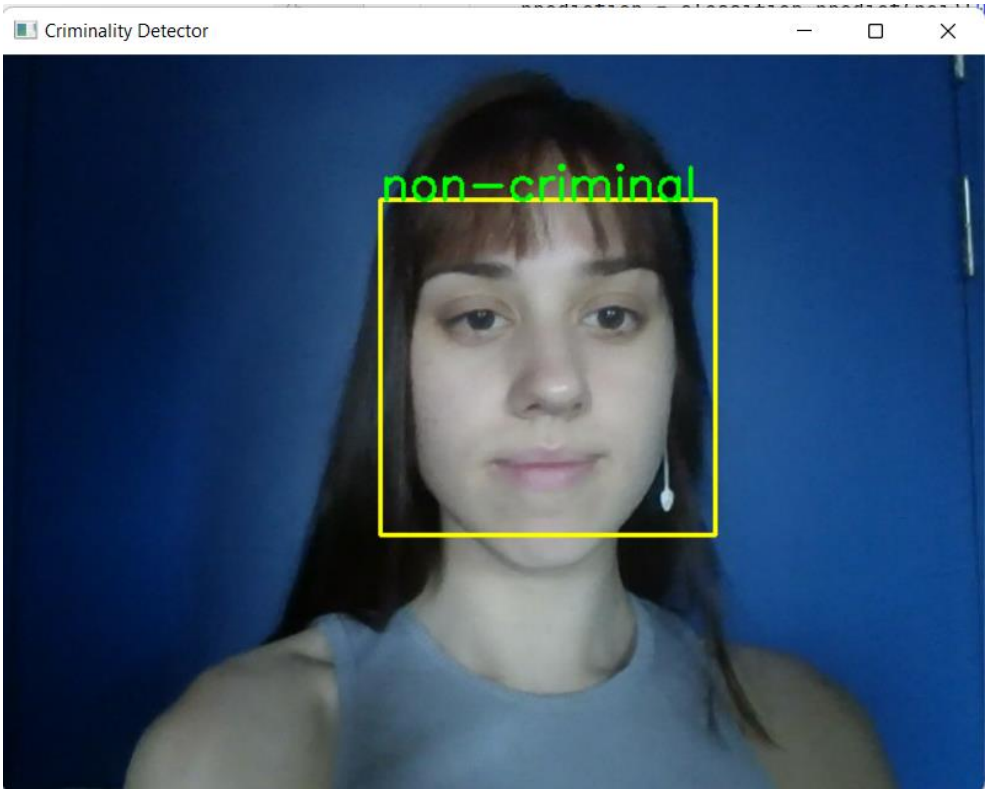


Рис. 4.2. Приклад роботи програми

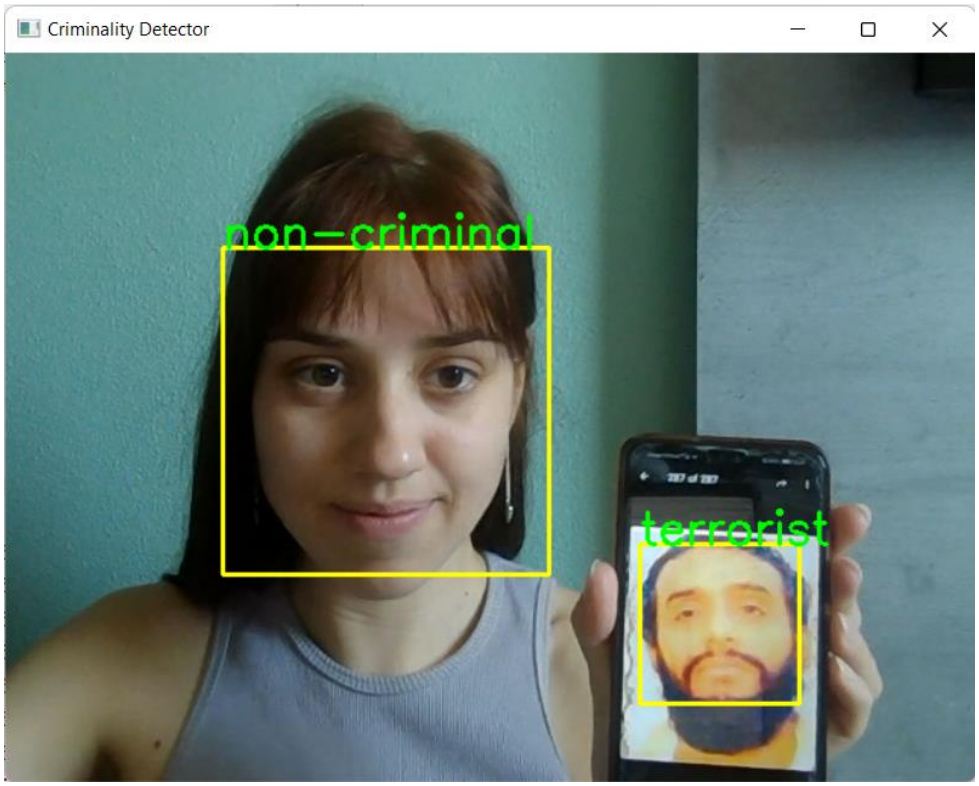


Рис. 4.3. Приклад роботи програми

Переходячи до практичної реалізації програми, зауважу її основну ціль – загальне підвищення точності розпізнавання обличь для контролювання місцевості у публічних місцях.

В останні роки біометричні методи виявилися найбільш перспективним варіантом розпізнавання осіб. Ці методи досліджують фізіологічні та поведінкові характеристики індивіда, щоб визначити та з'ясувати його особу, а не автентифікувати людей і надавати їм доступ до фізичних доменів за допомогою паролів, PIN-кодів, смарт-карт, пластикових карток, жетонів або ключів. Паролі та PIN-коди важко запам'ятати, їх можна легко вкрасти або вгадати; картки, жетони, ключі тощо можуть бути втрачені, забуті, викрадені чи скопійовані; магнітні картки можуть пошкодитися і стати нечитабельними. Проте біологічні риси особистості не можна втратити, забути, вкрасти чи підробити [1]. Розпізнавання обличь є однією з найменш нав'язливих і найшвидших біометричних методів у порівнянні з іншими методами, такими як розпізнавання відбитків пальців і райдужної оболонки ока. Наприклад, у системах відеоспостереження замість того, щоб вимагати від людей покласти руки на пристрій для зчитування відбитків пальців або точно розташувати очі перед сканером (розпізнавання райдужної оболонки), системи розпізнавання обличь ненав'язливо фотографують обличчя людей, коли вони входять у визначену зону. площа. Немає вторгнення чи затримки захоплення, і в більшості випадків суб'єкти зовсім не знають про процес. Люди не обов'язково відчувають, що під наглядом чи вторгнення в їхнє приватне життя [2], [3].

Завдяки використанню в кількох програмах розпізнавання обличь привернуло значну увагу як дослідницьких спільнот, так і ринку, і з'явився попит на надійні алгоритми розпізнавання обличь, які можуть працювати з реальними зображеннями обличчя [4], [5]. Щоб підтвердити гіпотезу про зростання публікацій з розпізнавання обличь, за допомогою Google Scholar

виконується проста вправа. Ми шукали опубліковані статті та патенти, що містять слова «розпізнавання обличчя» та «патенти на розпізнавання обличчя» протягом кожного року з 2000 по 2012 рік. На рис. 4.4 показано кількість опублікованих статей, а зареєстровані патенти на розпізнавання обличь за цей період. Необхідно зазначити, що цитування 2013 року ще не завершено, що пояснює, чому ми не включаємо 2013 рік у цю вправу.

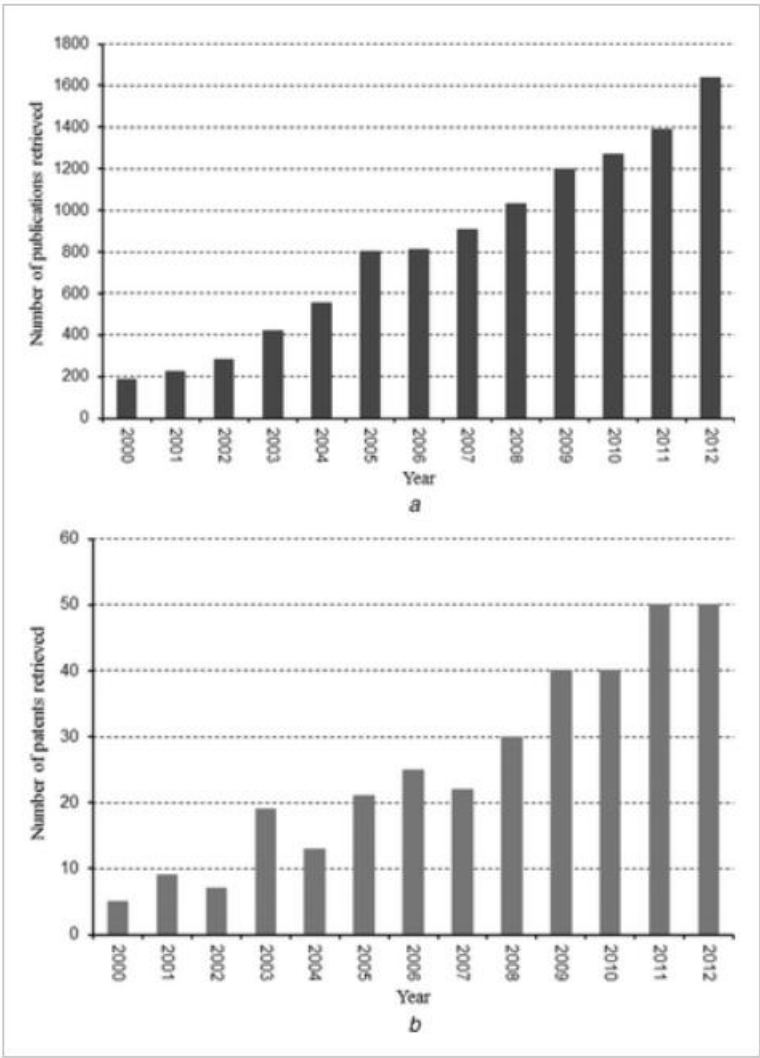


Рис. 4.4. Кількість опублікованих статей по РО

Приклади деяких проблем, які ще тільки виоішкються для поліршення точності алгоритмів розпізнавання:

- проблеми через зміни освітлення;
- проблеми через різницю поз/точок зору;

- проблеми через вікові зміни;
- проблеми через вираз обличчя/стиль обличчя;
- проблеми через оклюзію.

Проблеми, пов’язані з отриманням зображень і умовами зображення, були в центрі уваги досліджень розпізнавання обличчя протягом десятиліть, але вони досі не вирішені належним чином. Жодна поточна система не може стверджувати, що добре справляється з усіма цими проблемами, і жоден з поточних алгоритмів не є на 100% правильним, оскільки продуктивність поточних систем розпізнавання обличчя все ще дуже чутлива до будь-якої мінливості в зона обличчя. Крім того, розпізнавання обличь являє собою постійний набір ключових наукових проблем. Наприклад, велика кількість популярних методів розпізнавання обличчя зазвичай передбачає наявність кількох зразків для кожної людини, доступних для виділення ознак на етапі навчання. Однак у реальних програмах розпізнавання обличчя, таких як покращення законодавства та ідентифікація ідентифікаційної картки, це припущення може не спрацьовувати, оскільки в цих системах записується лише один зразок на людину.

Крім того, виділення надійних і дискримінантних ознак, які роблять внутрішньоособисті обличчя компактними і збільшують межі між різними особами, є важливою і складною проблемою в області розпізнавання обличчя [12], [82]). Більше того, як ми можемо зрівняти або перевищити продуктивність людського обличчя при виконанні завдань розпізнавання обличь у реальному світі (наприклад, розпізнавання людей, відомих глядачу)? Як ми можемо дізнатися гарну модель обличчя з невеликої кількості прикладів? Як ми можемо досягти рівня надійності, який демонструє розпізнавання людського обличчя? Як ми можемо зробити розпізнавання обличь стійким до наслідків старіння облич? Ці питання та постійно зростаючий попит на технологію обіцяють підтримувати

розпізнавання обличчя активним протягом тривалого часу в майбутньому [17].

4.2. Алгоритм використання інформаційного забезпечення прогнозування

У багатьох опублікованих роботах згадуються численні програми, в яких уже використовується технологія розпізнавання обличь, включаючи вхід і вихід у захищені місця з високим рівнем ризику, такі як перетини кордону, військові бази та атомні електростанції, а також доступ до обмежених ресурсів, таких як комп'ютери, мережі, персональні пристрої. , банківські операції, торгові термінали та медична документація [1], [6], [24]. З іншого боку, є й інші сфери застосування, в яких розпізнавання обличь ще не використовується; крім того, нинішні комерційні ринки поки що лише підряпали поверхню потенціалу. Потенційні сфери застосування технології розпізнавання обличчя окреслені нижче.

Автоматизоване спостереження, метою якого є розпізнавання та відстеження людей, які перебувають у списку спостереження. У цій програмі відкритого світу системі поставлено завдання розпізнати невелику групу людей, відкидаючи всіх інших як одні з розшукуваних [25].

Моніторинг замкненого телебачення (CCTV), можливість розпізнавання обличь може бути вбудована в існуючі мережі відеоспостереження, щоб шукати відомих злочинців або злочинців, пов'язаних з наркотиками, а потім органи влади можуть бути повідомлені, коли вони знайдені. Іншими словами, якщо використовується система розпізнавання обличь, вона може попереджати владу про наявність відомих або підозрюваних терористів або злочинців, чиї зображення вже зареєстровані в галереї. Крім того, його можна використовувати для розшуку втрачених дітей або інших зниклих безвісти.

Дослідження в базі зображень, пошук у базах даних зображень водіїв, отримувачів пільг, іммігрантів і поліцейських звернень, пошук людей у великих колекціях фотографій і відео новин [26], [27], а також пошук на веб-сайті соціальної мережі Facebook [28].

Мультимедійні середовища з адаптивними людськими комп'ютерними інтерфейсами (частина повсюдних або контекстно-залежних систем, моніторинг поведінки в дитячих садках чи центрах для літніх людей, розпізнавання клієнтів та оцінка їхніх потреб) [22].

Вихід на посадку в літак, розпізнавання обличчя може використовуватися в місцях вибіркових перевірок лише для перевірки пасажирів для подальшого розслідування. Аналогічно в казино, де стратегічний дизайн майданчиків для ставок, який включає камери на висоті обличчя з хорошим освітленням, може використовуватися не тільки для сканування обличь з метою ідентифікації, але, можливо, і для отримання зображень для створення всеосяжної галереї для майбутнього списку спостереження, завдання ідентифікації та аутентифікації [29].

Реконструкція обличь на основі ескізу, коли правоохоронні органи у світі покладаються на практичні методи, щоб допомогти свідкам злочинів відновити схожість обличь [30]. Ці методи варіюються від майстерності ескізів до власних комп'ютеризованих композитних систем [31]-[33].

Криміналістичні програми, коли криміналіста часто використовують для роботи з очевидцем, щоб намалювати ескіз, який зображує зовнішність винного відповідно до його/її словесного опису. Цей криміналістичний ескіз пізніше використовується для порівняння великих баз даних зображень обличчя для ідентифікації злочинців [34], [35]. Тим не менш, не існує існуючої системи розпізнавання облич, яку можна було б використовувати для ідентифікації або перевірки під час розслідування злочинів, наприклад, порівняння зображень, зроблених камерою відеоспостереження, з доступною базою даних фотографій. Таким чином, використання технології

розпізнавання обличь у криміналістичних програмах є обов'язковим, як обговорено в [7], [36].

Спуфінг та запобігання спуфінгу, коли фото чи відео обличчя уповноваженої особи можна використовувати для отримання доступу до засобів чи послуг. Отже, підробна атака полягає у використанні підроблених біометричних ознак для отримання нелегітимного доступу до захищених ресурсів, захищених системою біометричної аутентифікації [37], [38]. Це пряма атака на сенсорний вхід біометричної системи, і зловмиснику не потрібні попередні знання про алгоритм розпізнавання. Дослідження виявлення підробки обличчя останнім часом привертають все більшу увагу [39], запроваджуючи кілька методів виявлення підробок [40]-[42]. Таким чином, розробка зрілого алгоритму захисту від спуфінгу все ще знаходиться на зародковому етапі, і необхідні подальші дослідження для додатків для спуфінгу [51].

4.3. Заходи для можливого використання інформаційного забезпечення для правових структур

Технологія розпізнавання обличь — це лише один із набору нових цифрових інструментів, які впроваджують поліція та інші постачальники послуг безпеки в усьому світі, щоб функціонувати безпечніше та ефективніше. Тобто населення зараз знаходиться в стадії звикання до подібних технологій. Не треба додавати, що до введення описаної в роботі технології треба підходити ще більш обережно.

Розглянемо результати дослідження, проведеного в Лондоні, що вивчає реакцію громадськості на Live Facial Recognition (LFR): технологію, яка дозволяє поліції здійснювати автоматичну перевірку особи в громадських місцях у реальному часі. Я вважаю, що громадська довіра та легітимність є важливими факторами, які передбачають прийняття чи відмову від LFR. Найважливішим є те, що довіра та, зокрема, законність,

здається, допомагають пом’якшити занепокоєння щодо конфіденційності щодо використання поліцією цієї технології. В епоху, коли поліція використовує нові технології, імовірно, лише зростатиме, особливо в міру розвитку глобальної пандемії Covid-19, ці висновки мають важливе значення для відносин між поліцією та громадськістю та того, як «голос громадськості» використовується в дебатах.

Поліція та інші постачальники послуг безпеки в країнах по всьому світу все частіше звертаються до нових технологій, щоб більш безпечно та ефективно виконувати основні функції та боротися зі швидко мінливим ландшафтом загроз, шкоди та викликів. Фізичні технології, як-от дрони, GPS та вдосконалене обладнання для сканування, використовуються все більше і більше разом із програмним забезпеченням, таким як алгоритми «прогнозної поліції» та «великі дані». Використання цих технологій може по-різному формувати відносини між поліцією та громадськістю, але в багатьох випадках ці події відбувалися без значного суспільного розбрату чи навіть дебатів. Чи є це результатом широкої підтримки використання поліцією таких нових технологій, можливо, зумовленої довірою та інституційною легітимністю та/або тривогою щодо злочинності? Чи пов’язана відсутність дискусій із поміркованого прийняття перед обличчям швидких технологічних змін у суспільстві чи простого браку знань та поінформованості про проблеми? Про ці питання напрочуд мало відомо.

Технологія LFR виявилася однією з найбільш політичних проблем у поліцейській діяльності за останні роки, викликаючи значні дискусії в пресі та громадськості та принаймні дві юридичні проблеми. Результати представленого тут дослідження, здається, підтверджують ідею про те, що це область значних розбіжностей: наприклад, як стверджує лондонське дослідження [52], коли людям було запропоновано основне запитання про те, чи нормально для поліції використовувати LFR, респонденти розділилися майже 50/50. Довіра громадськості і, зокрема, легітимність

поліції були важливими факторами, які сформували прийняття або відмову від цієї поліцейської технології. Найважливішим є те, що законність, зокрема, служила для того, щоб пом'якшити, приглушити або, можливо, просто обійти проблеми конфіденційності. Інакше кажучи і зворотні формулювання, наведені вище, люди, які менше довіряють поліції і надають меншу легітимність, як правило, мають підвищену стурбованість щодо конфіденційності, і така занепокоєння дуже сильно пов'язана з поглядом, що це неприйнятно для поліції. використовувати LFR. Цікаво, але, мабуть, не дивно, що судження про поліцію є набагато важливішими провісниками визнання, ніж занепокоєння щодо злочинності, припускаючи, що афективний зв'язок — або його відсутність — з тими, хто використовує технологію (тобто поліцією) важливіший за цілі. на яку вона орієнтована.

З іншого боку, очевидна важливість довіри та законності для формування суджень людей у цій сфері вказує на важливі обмеження в тому, наскільки схвалення чи несхвалення громадськості є відповідним показником, за яким можна судити про доцільність діяльності поліції. Це найбільш чітко приділяється уваги в нашому обговоренні впливу легітимності як обов'язку підкорятися. Якщо це правда, що почуття морального обов'язку підкорятися поліції передбачає пасивне прийняття поліцейської діяльності, то це говорить про те, що люди виносять не етичне рішення, не кажучи вже про юридично чи політично поінформоване, а просто передають поліцейським здатність виконувати діяти як хочуть. Справді, така «авторизація» може розглядатися як центральна для концепції легітимності, принаймні, як це теоретизували деякі. Розширення повноважень поліції на основі відчуття нормативної відповідності може мати приблизно такий самий ефект, навіть якщо психологічний механізм, який діє, досить інший. Відверто кажучи, довіра та легітимність, яку вона створює, можуть спонукати деяких людей підтримувати діяльність поліції,

яка об’єктивно викликає занепокоєння, є недоречною або явно неправильною.

Будь-яке подібне занепокоєння має бути пом’якшене тим фактом, що законність міцно ґрунтується на справедливих судженнях, і існує безліч доказів, які свідчать про те, що несправедлива практика може мати значні наслідки, що в кінцевому підсумку призведе до відкликання згоди, а іноді й до радикальних змін. Крім того, з’являється консенсус, що, виносячи судження щодо законності, люди думають про те, чи відбувається діяльність поліції у відповідних юридичних та етичних межах, і що легітимність страждає, коли такі межі переходять. У зв’язку з цим, нещодавні дослідження показали, що легітимність сприяє підтримці дій з нормативно відповідними межами, але не діяльності, наприклад надмірного застосування сили, яка їх порушує. Таким чином, легітимність та процеси, які її підтримують, не забезпечують карт-бланш, а скоріше існують у динамічній напрузі з діяльністю та політикою поліції, інколи надаючи підтримку, а іноді гальмуючи або спричиняючи зміну напрямку.

4.4. Висновки після четвертого розділу

У ході четвертого розділу було показано інтерфейс для роботи з програмою. Описано майбутні задачі для підвищення точності, описано основні проблеми. Показано основні сфери застосування механізму. Розпізнавання обличь є складною проблемою в області комп’ютерного зору, якій протягом останніх років приділено велику увагу через кілька застосувань у різних областях. Незважаючи на те, що в цій області активно проводяться дослідження, створюючи зрілі системи розпізнавання обличь для роботи в обмежених умовах, вони далекі від досягнення ідеалу здатності адекватно працювати в усіх різних ситуаціях, з якими зазвичай стикаються програми в реальному світі. Цей розділ служить орієнтиром для об’єктивної оцінки прогресу спільноти в дослідженнях розпізнавання

обличь і для кращого вирішення проблем розпізнавання обличь у реальних сценаріях. Було розглянуто поточні досягнення в області розпізнавання обличь і обговорено кілька проблем і ключових факторів, які можуть суттєво вплинути на продуктивність систем розпізнавання обличь. Крім того, частина розділу спрямована на використання технології розпізнавання обличчя в інших наукових і повсякденних сферах життя.

Також було показано, що не останню роль відіграє сприйняття подібних технологій населенням для його впровадження.

ВИСНОВКИ

Класифікація людей будь-яким чином вимагає обережності, але прогнозування того, чи є особа злочинцем та яким саме, вимагає ще більшої обережності та ретельного огляду, і на цю класифікацію треба докладати максимальну кількість зусиль. Небезпека цієї технології полягає в її недосконалості, оскільки неправильна класифікація осіб може мати серйозні наслідки. Було б занадто оптимістично стверджувати, що 73% точності тесту, досягнутої CNN у цій роботі, легко можна узагальнити на знімки обличчя з будь-якого іншого джерела. Це пов’язано не лише з невеликим розміром нашого набору даних, а й із тим, що кримінальні та некримінальні зображення надходять із різних джерел. Таким чином, умови, за яких знімаються зображення, не зовсім однакові, що породжує питання, чи була ця невідповідність периферійних умов зафіксована глибоким класифікатором, щоб точно розрізняти два класи. В ідеальному наборі даних усі знімки обличчя, кримінальні та некримінальні, будуть зроблені однією камерою та за однакових умов, тобто освітлення, кут, відстань, фон, якість зображення, макіяж, борода, капелюх та окуляри.

Емоції на обличчі та вік, основні джерела упередженості в класифікації зображень обличчя на основі кримінальної тенденції. Змішення через фонові ефекти було пом’якшено, обрізаючи область обличчя із зображень. Гендерну упередженість усунуто шляхом ігнорування жіночих образів. Раса, ще одне джерело упередженості, не була врахована в цьому дослідженні через невеликий набір даних та складність, а іноді й суб’єктивність ідентифікації раси за низькоякісними зображеннями обличчя.

Надалі обстеження можна повторити з більшою кількістю даних. Також дослідження може бути покращено шляхом вивчення не всієї зовнішності злочинців, а окремих особливостей, які відповідають за риси особистості Великої п'ятірки.

В майбутньому це робота може мати продовження у вигляді вивчення окремих наборів рис обличчя для кожної категорії.

Так як датасет був невеликий, першочергово треба повисити якість розпізнавання вже існуючих категорій, аде надалі розширення кількості класів для класифікації також є можливим.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Xiaolin Wu, Xi Zhang, Automated Inference on Criminality using Face Images, 2017. URL: https://arxiv.org/pdf/1611.04135.pdf.

2. Osin E., Novokshonov A., Shutilov K., Davydov D., Kachur A., Assessing the Big Five personality traits using real-life static facial images, 2020. URL: https://www.researchgate.net/publication/341568689_Assessing_the_Big_Five_personality_traits_using_real-life_static_facial_images.

3. Nurul Azma Abdullah, Md. Jamri Saidi, Nurul Hidayah Ab Rahman, Chuah Chai Wen, Isredza Rahmi A. Hamid, Face recognition for criminal identification: An implementation of principal component analysis for face recognition, 2017. URL: https://aip.scitation.org/doi/pdf/10.1063/1.5005335#:~:text=Face%20Recognition%20for%20Criminal%20Identification%20is%20a%20face%20recognition%20system,be%20removed%20from%20the%20image.

4. Hui Lv, Chuanwei Zhou, Chunyan Xu, Zhen Cui, Jian Yang, Localizing Anomalies from Weakly-Labeled Videos, 2020. URL: .https://arxiv.org/pdf/2008.08944v3.pdf

5. Alex Najibi. Racial Discrimination in Face Recognition Technology, 2020. URL: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

6. Global Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analytics), by Application (Access Control, Security & Surveillance), by End-use, by Region, and Segment Forecasts, 2020. URL: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market

7. Klare, Brendan & Park, Unsang. (2011). Face recognition: Some challenges in forensics. 2011 IEEE International Conference on Automatic Face and Gesture Recognition and Workshops, FG 2016. 726 - 733.

10.1109/FG.2011.5771338. URL: https://www.researchgate.net/publication/224238093_Face_recognition_Some_challenges_in_forensics

8. Ali, Tauseef & Veldhuis, Raymond & Spreeuwers, Luuk. (2017). Forensic Face Recognition: A Survey. Face Recognition: Methods, Applications and Technology. URL: https://www.researchgate.net/publication/48340425_Forensic_Face_Recognition_A_Survey

9. Interpol - Facial Recognition. URL: https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

10. Ben Hartwig. The Benefits and Drawbacks of Automated Facial Recognition in Forensic Science, 2020. URL: https://www.technologynetworks.com/applied-sciences/articles/the-benefits-and-drawbacks-of-automated-facial-recognition-in-forensic-science-341401

11. Nicole A. Spaun. Face Recognition in Forensic Science, 2020. URL: https://link.springer.com/chapter/10.1007/978-0-85729-932-1_26

12. UCF-Crime database. URL: https://www.crimemuseum.org/crime-library/forensic-investigation/facial-recognition-and-facial-reconstruction/#:~:text=Facial%20recognition%20and%20facial%20reconstruction,picture%20technology%20can%20be%20used%20.

13. Hui Lv, Chuanwei Zhou, Chunyan Xu, Zhen Cui, Jian Yang. Localizing Anomalies from Weakly-Labeled Videos, 2020. URL: https://paperswithcode.com/paper/localizing-anomalies-from-weakly-labeled

14. Amazon Rekognition FAQs. URL: https://aws.amazon.com/rekognition/faqs/

15. Sandeep Kulkarni and Kara Yang. Field Notes: Speed Up Redaction of Connected Car Data by Multiprocessing Video Footage with Amazon Rekognition, 2021. URL:

https://aws.amazon.com/blogs/architecture/field-notes-speed-up-redaction-of-connected-car-data-by-multiprocessing-video-footage-with-amazon-rekognition/

16. Peter Morrall. Murder and society: why commit murder?, 2020. URL: https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627250608553401.pdf

17. Authors: Nicola S. Gray, Malcolm J. MacCulloch, Jennifer Smith, Mark Morris and Robert J. Snowden. Forensic psychology: Violence viewed by psychopathic murderers, 2019. URL: https://go.gale.com/ps/i.do?id=GALE%7CA187717710&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00280836&p=HRCA&sw=w&userGroupName=anon%7E80371765

18. B Lia, K Skjølberg. Causes of Terrorism: An Expanded and Updated Review of the Literature, 2004. URL: https://gsdrc.org/document-library/causes-of-terrorism-an-expanded-and-updated-review-of-the-literature/

19. P. Howland, J. Wang, and H. Park, ‘‘Solving the small sample size problem in face recognition using generalized discriminant analysis,’’ Pattern Recognit., vol. 39, no. 2, pp. 277–287, Feb. 2006.

20. Y. He, ‘‘An efficient method to solve small sample size problem of LDA using householder QR factorization for face recognition,’’ in Proc. Int. Conf. Comput. Inf. Sci., Oct. 2011, pp. 79–82.

21. R. Gottumukkal and V. K. Asari, ‘‘An improved face recognition technique based on modular PCA approach,’’ Pattern Recognit. Lett., vol. 25, no. 4, pp. 429–436, Mar. 2004.

22. C. Cortes and V. Vapnik, ‘‘Support-vector networks,’’ Mach. Learn., vol. 20, no. 3, pp. 273–297, 1995.

23. Y. Freund, R. Iyer, E. R. Schapire, Y. Singer, and G. T. Dietterich, ‘‘An efficient boosting algorithm for combining preferences,’’ J. Mach. Learn. Res., vol. 4, no. 6, pp. 170–178, 2004.

24. L. I. Xiang-Feng, Z. Wei-Kang, D. Xin-Yuan, L. Kun, and Z. Dun-Wen, ‘‘Vehicle detection algorithm based on improved AdaBoost and Haar,’’ Meas. Control Technol., Feb. 2019.

25. Yamashita, R., Nishio, M., Do, R.K.G. *et al.* Convolutional neural networks: an overview and application in radiology. *Insights Imaging* **9,** 611–629 (2018). https://doi.org/10.1007/s13244-018-0639-9

26. Keiron O'Shea, Ryan Nash. An Introduction to Convolutional Neural Networks, 2017. URL: https://arxiv.org/pdf/1511.08458.pdf

27. Lin M, Chen Q, Yan S (2013) Network in network. arXiv. Available online at: https://arxiv.org/pdf/1312.4400.pdf. Accessed 22 Jan 2018

28. Qian N (1999) On the momentum term in gradient descent learning algorithms. Neural Netw 12:145–151

29. Kingma DP, Ba J (2014) Adam: a method for stochastic optimization. arXiv. Available online at: https://arxiv.org/pdf/1412.6980.pdf. Accessed 23 Jan 2018

30. Ruder S (2016) An overview of gradient descent optimization algorithms. arXiv. Available online at: https://arxiv.org/pdf/1609.04747.pdf. Accessed 23 Jan 2018

31. Nair V, Hinton GE (2010) Rectified linear units improve restricted Boltzmann machines. In: Proceedings of the 27th International Conference on Machine Learning. Available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.6419&rep=rep1&type=pdf. Accessed 23 Jan 2018

32. Ramachandran P, Zoph B, Le QV (2017) Searching for activation functions. arXiv. Available online at: https://arxiv.org/pdf/1710.05941.pdf. Accessed 23 Jan 2018

33. Glorot X, Bordes A, Bengio Y (2011) Deep sparse rectifier neural networks. In: Proceedings of the 14th International Conference on Artificial Intelligence and Statistics, vol 15, pp 315–323

34. LeCun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521:436–444

35. Krizhevsky A, Sutskever I, Hinton GE (2012) ImageNet classification with deep convolutional neural networks. Adv Neural Inf Process Syst 25. Available online at: https://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks.pdf. Accessed 22 Jan 2018

36. Nivedita Ray De Sarkar, Anirban Kundu, Mou De, Anupam Bera, Agent Based Noise Detection Using Real Time Data Analysis Towards Green Environment, International Journal of Green Computing, 10.4018/IJGC.2017070103, 8, 2, (37-58), (2017).

37. G. Betta, D. Capriglione, M. Corvino, C. Liguori, P. Sommella, undefined, 2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 10.1109/I2MTC.2017.7969704, (1-6), (2017).

38. Shiv Ram Dubey, Satish Kumar Singh, Rajat Kumar Singh, Local SVD based NIR face retrieval, Journal of Visual Communication and Image Representation, 10.1016/j.jvcir.2017.09.004, 49, (141-152), (2017).

39. Santosh Kumar, Sanjay Kumar Singh, Visual animal biometrics: survey, IET Biometrics, 10.1049/iet-bmt.2016.0017, 6, 3, (139-156), (2017).

40. Jou Lin, Ching-Te Chiu, Low-complexity face recognition using contour-based binary descriptor, IET Image Processing, 10.1049/iet-ipr.2016.1074, 11, 12, (1179-1187), (2017).

41. Arash Rikhtegar, Mohammad Pooyan, Mohammad Taghi Manzuri-Shalmani, Genetic algorithm-optimised structure of convolutional neural network for face recognition applications, IET Computer Vision, 10.1049/iet-cvi.2015.0037, 10, 6, (559-566), (2016).

42. Ithayarani Panner Selvam, Muneeswaran Karruppiah, Fusing the facial temporal information in videos for face recognition, IET Computer Vision, 10.1049/iet-cvi.2015.0394, 10, 7, (650-659), (2016).

43. Fatema Tuz Zohra, Md Wasiur Rahman, Marina Gavrilova, undefined, 2016 International Conference on Cyberworlds (CW), 10.1109/CW.2016.40, (189-196), (2016).

44. L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology," in IEEE Access, vol. 8, pp. 139110-139120, 2020, doi: 10.1109/ACCESS.2020.3011028.https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4

45. Peter Goldsborough. A Tour of TensorFlow, 2016. URL: https://arxiv.org/pdf/1610.01178.pdf

46. FBI Terrorism. URL: https://www.fbi.gov/wanted/terrorism

47. FBI Bank Robbers. URL: https://bankrobbers.fbi.gov/

48. FBI Fugitives. URL: https://www.fbi.gov/wanted/fugitives

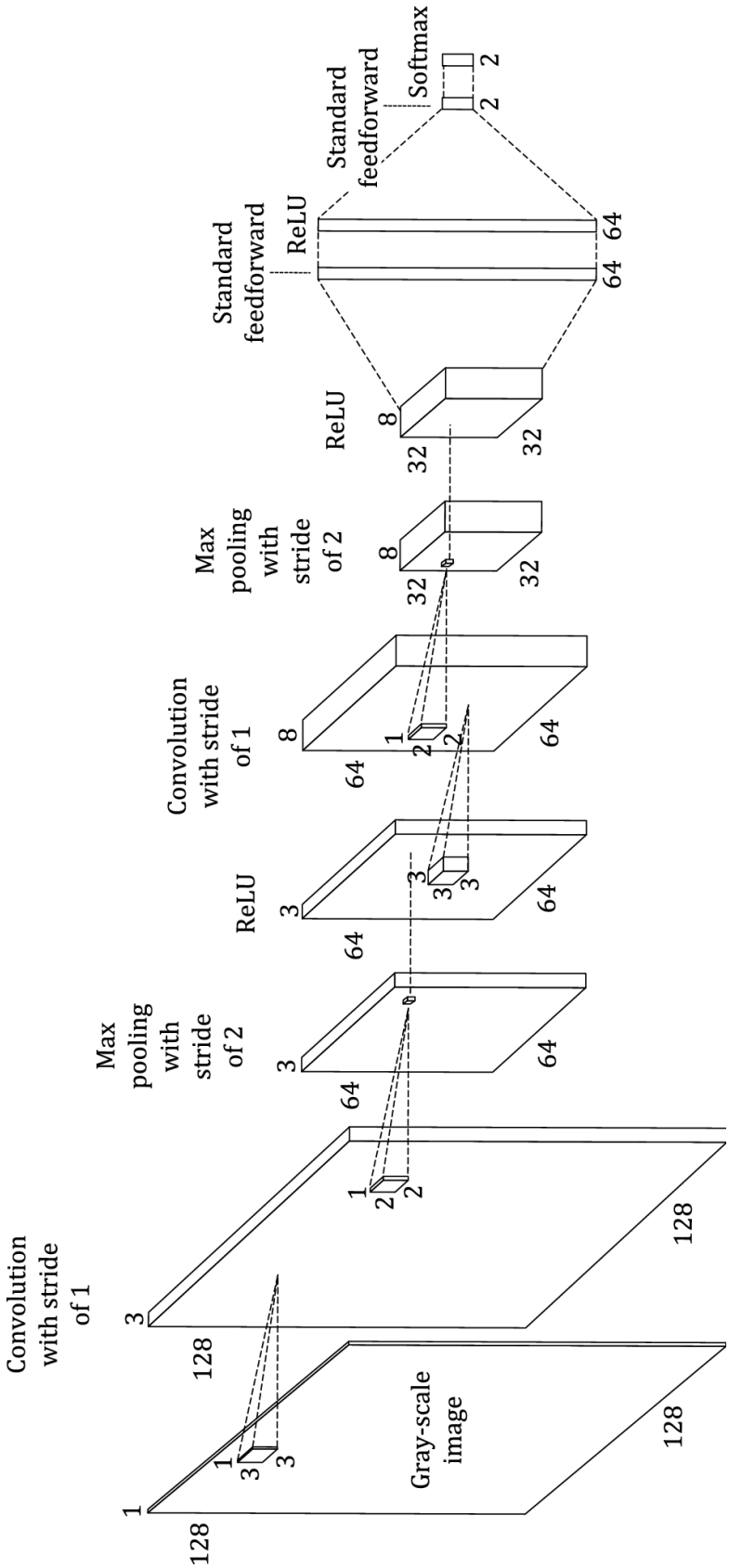
49. Interpol Red Notice. URL: https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices

50. M. Hassaballah, Saleh Aly. Face recognition: challenges, achievements and future directions, 2018. URL: https://doi.org/10.1049/iet-cvi.2014.0084

51. Ben Bradford, Julia A Yesberg, Jonathan Jackson, Paul Dawson. Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support For Police Use of New Technology, 2020. URL: https://academic.oup.com/bjc/article/60/6/1502/5843315?login=true

ДОДАТКИ

Додаток А. Схема нейронної мережі проекту.



Додаток Б. Код моделі

```
model = Sequential()

#1st CNN layer
model.add(Conv2D(64,(3,3),padding = 'same',input_shape = (48,48,1)))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size = (2,2)))
model.add(Dropout(0.25))

#2nd CNN layer
model.add(Conv2D(128,(5,5),padding = 'same'))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size = (2,2)))
model.add(Dropout (0.25))

#3rd CNN layer
model.add(Conv2D(512,(3,3),padding = 'same'))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size = (2,2)))
model.add(Dropout (0.25))

#4th CNN layer
model.add(Conv2D(512,(3,3),padding = 'same'))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size = (2,2)))
model.add(Dropout (0.25))

#5th CNN layer
model.add(Conv2D(512,(3,3), padding='same'))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size=(2, 2)))
model.add(Dropout(0.25))

model.add(Flatten())

#Fully connected 1st layer
model.add(Dense(256))
model.add(BatchNormalization())
model.add(Activation('relu'))
model.add(Dropout(0.25))


# Fully connected layer 2nd layer
model.add(Dense(512))
model.add(BatchNormalization())
model.add(Activation('relu'))
```

```
model.add(Dropout(0.25))

model.add(Dense(no_of_classes, activation='softmax'))
model.add(BatchNormalization())


opt = adam_v2.Adam(lr = 0.0001)
model.compile(optimizer=opt,loss='categorical_crossentropy', metrics=['accuracy'])
model.summary()

from keras.optimizers import adam_v2
from keras.callbacks import ModelCheckpoint, EarlyStopping, ReduceLROnPlateau

checkpoint = ModelCheckpoint("./model.h5", monitor='val_acc', verbose=1,
save_best_only=True, mode='max')

reduce_learningrate = ReduceLROnPlateau(monitor='val_loss',
                      factor=0.2,
                      patience=3,
                      verbose=1,
                      min_delta=0.0001)

callbacks_list = [early_stopping,checkpoint,reduce_learningrate]

early_stopping = EarlyStopping(monitor='val_loss',
                    min_delta=0,
                    patience=3,
                    verbose=1,
                    restore_best_weights=True
                    )

epochs = 15

model.compile(loss='categorical_crossentropy',
          optimizer = adam_v2.Adam(lr=0.001),
          metrics=['accuracy'])

#%%
history = model.fit_generator(generator=train_set,
                        steps_per_epoch=train_set.n//train_set.batch_size,
                        epochs=epochs,
                        validation_steps = test_set.n//test_set.batch_size,
                        callbacks=callbacks_list
                        validation_data = test_set,
)

plt.style.use('dark_background')
plt.suptitle('Optimizer : Adam', fontsize=10)
plt.ylabel('Loss', fontsize=16)
plt.plot(history.history['loss'], label='Training Loss')
plt.plot(history.history['val_loss'], label='Validation Loss')
```

```
plt.legend(loc='upper right')
plt.figure(figsize=(20,10))
plt.subplot(1, 2, 1)

plt.ylabel('Accuracy', fontsize=16)
plt.plot(history.history['accuracy'], label='Training Accuracy')
plt.plot(history.history['val_accuracy'], label='Validation Accuracy')

plt.subplot(1, 2, 2)
plt.legend(loc='lower right')
plt.show()
```

Додаток В. Код вікна класифікатора

```
cap = cv2.VideoCapture(0)



while True:
labels = []
    gray = cv2.cvtColor(frame,cv2.COLOR_BGR2GRAY)
    faces = face_classifier.detectMultiScale(gray)

    _, frame = cap.read()

    for (x,y,w,h) in faces:
        cv2.rectangle(frame,(x,y),(x+w,y+h),(0,255,255),2)
        roi_gray = gray[y:y+h,x:x+w]
        roi_gray = cv2.resize(roi_gray,(48,48),interpolation=cv2.INTER_AREA)



            prediction = classifier.predict(roi)[0]
            label=crime_labels[prediction.argmax()]
            label_position = (x,y)

        if np.sum([roi_gray])!=0:
            roi = roi_gray.astype('float')/255.0
            roi = img_to_array(roi)
            roi = np.expand_dims(roi,axis=0)

cv2.putText(frame,label,label_position,cv2.FONT_HERSHEY_SIMPLEX,1,(0,255,0),2)
        else:
cv2.imshow('Criminality Detector',frame)
            cv2.putText(frame,'No Faces',(30,80),cv2.FONT_HERSHEY_SIMPLEX,1,(0,255,0),2)
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break

cap.release()
```

Додаток Г. Код головного вікна

```
import tkinter as tk
from tkinter import font as tkFont
import analyzer
import trainer
import constants


def main():
    root = tk.Tk()
    root.geometry("+250+25")
    root.title('Аналіз зовнішності на предмет схильності до правопорушень')
    root.resizable(False, False)

    canvas = tk.Canvas(root, height=constants.HEIGHT, width=constants.WIDTH)
    canvas.pack()

title_font = tkFont.Font(family='Fixedsys', size=20)
    title = tk.Label(frame_title, text="ВІТАЄМО\nв аналізаторі зовнішності\nна предмет
схильності\nдо правопорушень", bg=constants.FRAME_BG,
                     font=title_font, fg=constants.FONT_COLOR, justify='left')
    title.place(relwidth=0.5, relheight=1)

    frame_button = tk.Frame(frame_title, bg=constants.FRAME_BG)
    frame_button.place(relwidth=0.5, relheight=0.8, relx=0.5, rely=0.1)

    button_font = tkFont.Font(family='Helvetica', size=14)



    bg_image = tk.PhotoImage(file=constants.BG_IMAGE)
    bg_label = tk.Label(root, image=bg_image)
    bg_label.place(relwidth=1, relheight=1)

    frame_title = tk.Frame(root, bg=constants.FRAME_BG)
    frame_title.place(relwidth=0.8, relheight=0.5, relx=0.1, rely=0.2)



    button_test = tk.Button(frame_button, text="ТРЕНУВАТИ модель",
bg=constants.BUTTON_1, bd=1, fg=constants.FONT_COLOR, font=button_font,
                            highlightbackground='#003347', command=trainer.create_trainer_window)
    button_test.place(relwidth=0.8, relheight=0.2, relx=0.1, rely=0.25)

    button_train = tk.Button(frame_button, text="АНАЛІЗУВАТИ обличчя real-time",
bg=constants.BUTTON_2, bd=1, fg=constants.FONT_COLOR, font=button_font,
                             highlightbackground='#661d07',
command=analyzer.create_analyzer_window)
    button_train.place(relwidth=0.8, relheight=0.2, relx=0.1, rely=0.55)
```

```
    # ################
    frame_executors = tk.Frame(root, bg=constants.FRAME_BG)
    frame_executors.place(relwidth=0.8, relheight=0.05, relx=0.1, rely=0.95)

    label_font = tkFont.Font(family='Helvetica', size=12)
    label = tk.Label(frame_executors, text='Створено Анастасією Мудрою ІАВ-21',
                     fg='#dbdbdb', bg=constants.FRAME_BG, font=label_font)
    label.place(relwidth=1, relheight=1)

    root.mainloop()

main()
```