Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра _____Автоматизації проектування обчислювальної техніки_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
_____Система розпізнавання відбитків пальців за допомогою нейронної_____
_____мережі з багатошаровою структурою_____
(тема)

Виконав: здобувач другого року навчання,
групи ___СКСм-24-1_____
_____Дубінник Є. О._____
(прізвище, ініціали)
Спеціальність _____
_____123– Комп'ютерна інженерія_____
(код і повна назва спеціальності)
Тип програми ____освітньо-професійна___
(освітньо-професійна або освітньо-наукова)
Освітня програма _____
___Спеціалізовані комп'ютерні системи___
(повна назва освітньої програми)
Керівник _____доц. Рожнова Т.Г._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ __Чумаченко С.В.___
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління_____
Кафедра_____Автоматизації проектування обчислювальної техніки_____
Рівень вищої освіти_____другий (магістерський)_____
Спеціальність_____123 Комп'ютерна інженерія_____
(код і повна назва)
Тип програми _____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма_____Спеціалізовані комп'ютерні системи_____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«_02_»_____09_____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
здобувачеві_____Дубіннику Єгору Олексійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи _____Система розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою_____
затверджена наказом університету від 07_____11_____2025 р. № _1012 Ст_
2. Термін подання здобувачем роботи до екзаменаційної комісії _24_ ____12____ 2025 р.
3. Вихідні дані до роботи _____
Архітектура нейронної мережі
Мова програмування Python
Середовище розробки MatLab
Бібліотека TensorFlow, PyTorch і Keras
Датасет з 4000 фотографій у форматі .png

4. Перелік питань, що потрібно опрацювати в роботі_____
1. Аналіз сучасних систем та технологій контролю доступу
2. Аналіз актуальних методів біометрчної ідентифікації
3. Дослідження сучасних нейромереж з багатошаровою структурою
4. Розробка моделі системи розпізнавання відбитків пальців на основі нейронної мережі

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
16 слайдів (формату .pptx)

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання за темою	01.09.2025-02.09.2025	
2	Аналіз предметної області	03.09.2025-15.09.2025	
3	Аналіз існуючих рішень	16.09.2025-09.10.2025	
4	Аналіз технологій обробки зображень	10.10.2025-15.10.2025	
5	Підбір навчальної вибірки для проведення дослідження	16.10.2025-20.10.2025	
6	Написання програмної реалізації розробленої моделі нейронної мережі	21.10.2025-25.11.2025	
7	Проведення дослідження ефективності моделі	26.11.2025-05.12.2025	
8	Оформлення пояснювальної записки	06.12.2025-10.12.2025	
9	Оформлення графічного матеріалу	10.12.2025-15.12.2025	
10	Перевірка роботи керівником	16.12.2025-20.12.2025	
11	Подання роботи до ЕК для захисту	22.12.2025-24.12.2025	

Дата видачі завдання 02.09.2025

Здобувач _____
(підпис)

Керівник роботи _____ Доцент кафедри АПОТ Рожнова Т.Г.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 63 сторінок, 27 рисунків, 4 таблиці, 23 джерела за переліком посилань.

НЕЙРОННА МЕРЕЖА, БАГАТОШАРОВА СТРУКТУРА, СИСТЕМА РОЗПІЗНАВАННЯ ОБРАЗІВ, БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ, СЕГМЕНТАЦІЯ, ВІДБИТКИ ПАЛЬЦІВ

Метою роботи є дослідження системи розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою.

Предметом дослідження є існуючи системи розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою та методи і техніки машинного розпізнавання відбитків пальців.

Об’єкт дослідження – процеси розпізнавання відбитків пальців за допомогою нейронної мережі для системи доступу.

Досліджено відомі архітектури нейронних мереж, з багатошаровою структурою, такі як MLP, CNN, RNN та їх модифікації BRNN, GRUs, LSTM. Досліджено методи і алгоритми обробки цифрових зображень та можливості машинного навчання для розпізнавання зображення відбитків пальців. Розроблено математичну модель аналізу ефективності роботи системи розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою.

ABSTRACT

The explanatory note to the qualification work contains : 63 pages, 27 figures 4 tables, 23 sources according to the list of references

NEURAL NETWORK, MULTILAYER STRUCTURE, PATTERN RECOGNITION SYSTEM, BIOMETRIC IDENTIFICATION, SEGMENTATION, FINGERPRINTS

The aim of the work is to study a fingerprint recognition system using a neural network with a multilayer structure.

The subject of the research is existing fingerprint recognition systems using a neural network with a multilayer structure and methods and techniques of machine fingerprint recognition .

The object of research is the processes of fingerprint recognition using a neural network for an access system.

Known architectures of neural networks with a multilayer structure, such as MLP, CNN, RNN and their modifications BRNN, GRUs, LSTM, are studied. Methods and algorithms for processing digital images and the capabilities of machine learning for fingerprint image recognition have been studied. A mathematical model for analyzing the efficiency of a fingerprint recognition system using a neural network with a multilayer structure has been developed.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CANNY EDGE DETECTOR – оператор виявляння контурів

CNN – згорткова нейронна мережа;

DP – глибоке навчання;

DQN – глибока Q-нейронна мережа;

LSTM – мережа довгої короткострокової пам’яті;

MEMS – мікроелектромеханічні системи;

MFCCs – Mel-frequency cepstral coefficients – це коефіцієнти мел-частотного кепстру, мел-шкала – це емпірична шкала, що спирається на відчуття частоти звуку людиною;

MFA – багатофакторна автентифікація;

NMS – non max suppression – це метод, що використовується переважно у виявленні об'єктів за допомогою обмежувальної рамки;

RNN – рекурентна нейронна мережа;

ЗНМ – згорткова нейронна мережа;

ОЯЗ – оцінювання якості зображень;

ШІ – штучний інтелект;

ШНМ – штучна нейронна мережа.

ВСТУП

У сучасному світі безпека контролю доступу понад усе, адже в нашому смартфоні практично все наше життя у вигляді платіжних карток, приватних фото, особисті переписки та бізнес. Сьогодні з метою забезпечення безпеки все частіше застосовуються біометричні технології в системах контролю доступу. Найбільш популярною біометричною технологією є технологія ідентифікації особистості за відбитками пальців та за обличчям

Біометричні системи контролю доступу надають можливість доступу за допомогою ідентифікації за відбитками пальця, сітківки ока, райдужної оболонки ока, формою долоні та формою обличчя. Окрім безпеки доступу такі системи дозволяють здійснювати облік робочого часу співробітників на підконтрольному об'єкті.

Стрімкий розвиток обчислювальних технологій дозволив технологіям, що потребують обчислення великих об’ємів даних, таким як ідентифікація за відбитками пальців, потрапити вряд автоматизованих технологій. Зовнішні характеристики відбитків пальців, що є особливими для кожної людини, стали характерними ознаками, за якими проводиться ідентифікація особи. Ідентифікація в такий спосіб є популярною через легкість використання цього методу. Вперше ідентифікація за відбитками стала розповсюдженою практикою завдяки серу Френсісу Гальтону, який в1888 році винайшов характеристики, за якими можна відрізнити відбитки пальців різних людей, так візерунок папілярних ліній став характеристикою для ідентифікації людини за відбитком пальців і основою науки дактилоскопії ще в позаминулому столітті.

Розвиток технологій у сфері штучного інтелекту, підштовхнув до вдосконалення в методології розпізнавання відбитків пальців, нейронні мережі стали інструментом в системах контролю доступу при розв’язанні завдання розпізнавання відбитків пальців та продемонстрували великий

потенціал у підвищенні точності біометричної аутентифікації для сучасних систем швидкого реагування та пристроїв із біометричними можливостями, що інтегруються в різні сфери нашого життя.

Кваліфікаційна робота присвячена дослідженню систем розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою для біометричної аутентифікації із обробкою великого обсягу шаблонів даних папілярних ліній відбитків пальців.

Таке дослідження є актуальним бо ідентифікація особи за відбитками пальців із використанням нейронних мереж підвищує точність та надійність систем біометричної аутентифікації та є зручною функцією у повсякденному використанні людини при використанні мобільних додатків.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ КОНТРОЛЮ ДОСТУПУ

1.1 Скорочена історія розвитку систем контролю доступу

Першим прототипом системи контролю доступу був замок, а типом даних ідентифікації, що використовуються для систем безпеки доступу, були замок та ключ, що використані людством у Месопотамії приблизно 4000 до нашої ери. Принцип роботи таких примітивних систем контролю доступу э схожим за своєю суттю на роботу існуючих в наш час, за час розвитку більше 60 століть технології і вигляд самих ключів стали різноманітніше та трошечки складнішими. Електронна система контроля доступу за допомогою нового типу ключа (пароль або карта RFID) змінює звичайний замок на електронний, а ключ змінює своє обличчя на цифрову комбінацію ключів та паролів для автентифікації користувача такої системи-замка.

Поштовхом до створення нової концепції ключів даних для таких систем контролю у 2000-х роках надали мобільні пристрої, для аутентифікації користувачів представлено мобільні картки аутентифікації, що мають технологічно вищій рівень безпеки для перевірки особи користувача за RFID карткою з прошитим унікальним номером. Але і такі карти не виключили повністю проблеми безпечного доступу в мобільних системах, самі ж мобільні пристрої з різними вбудованими системами такими як Bluetooth, що призначені для бездротового обміну даними на коротких відстанях, можуть створювати небезпеку для захисту паролів і самих карт під час такого передавання. Технологія біометрія, яка спирається на біометричні характеристики особи , надає нового розвитку системам контроля доступу , та є безпечнішою за RFIDкартки вході процесу ідентифікації.

Під час пандемії 2020 року виходять в світ ще одне рішення ключів до систем контролю доступу – це безконтактні на основі ШІ пристрої, при

використанні яких не потрібен фізичний контакт для процесу ідентифікації. Так розвиваються системи розпізнавання обличчя з підтримкою штучного інтелекту.

Мобільні програми автентифікації є останнім кроком, на даний час, в еволюції процесу отримання даних для систем контролю доступу. З огляду на те, що iPhone та смартфон використовуються особисто, то визнаємо, що мобільні карти смартфона є надійнішим посвідченням особи. Таким чином відносно, усунуті ризики небезпеки несанкціонованого використання особистих даних. Розпізнавання обличчя та мобільні додатки на основі штучного інтелекту є новою сходинкою розвитку технологій отримання даних для систем контролю доступу. Нам залишається спостерігати, що буде далі або прийняти, безпосередньо, участі в розвитку нових технологій ідентифікації для систем контролю доступу.

1.2 Система біометричної автентифікації за технологія Face ID

Технологія Face ID від Apple – це система біометричної автентифікації, яка використовує камеру True Depth та інфрачервоні датчики для створення D-карти обличчя користувача, розпізнає його за унікальними особливостями, що дозволяє розблокувати пристрій; здійснювати платежі Apple Pay та надає доступ до захищених програм. Така система працює шляхом проектування тисяч невидимих точок, створення інфрачервоного зображення та порівняння його з збереженим шаблоном, що забезпечує безпеку та зручність використання (рис.1.1).

В основі технології Face ID лежить система камер TrueDepth, розташована у верхній частині пристрою (Dynamic Island), яка об'єднує декілька високотехнологічних апаратних і програмних компонентів [1]:

– проектор точок Dot Projector, проєктує на обличчя користувача понад 30 тисяч невидимих інфрачервоних точок;

– інфрачервона камера, зчитує унікальний малюнок цих точок, створюючи структурну (3D) карту обличчя;

– інфрачервоний випромінювач Flood Illuminator, забезпечує роботу системи навіть у повній темряві, підсвітлюючи обличчя невидимим інфрачервоним світлом;

– нейронні мережі – отриманий математичний образ обличчя обробляється нейронними мережами в захищеному анклаві Secure Enclave процесора пристрою.

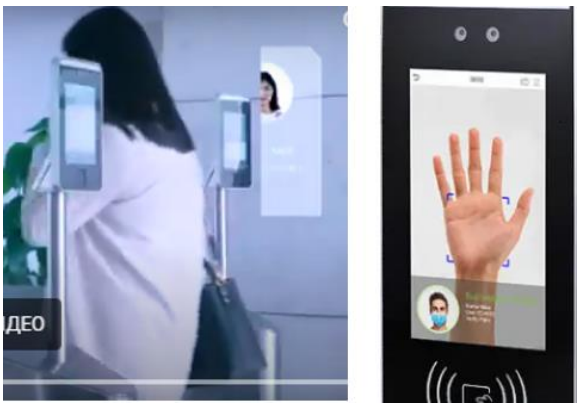


Рисунок 1.1 – Камера True Depth та інфрачервоні датчики для створення 3D-карти обличчя користувача

Під час кожного використання Face ID система порівнює поточну 3D-карту обличчя зі збереженим шаблоном, технологія самонавчається і здатна розпізнавати зміни в зовнішності: окуляри, макіяж, відросла борода, або навіть використання маски, постійно оновлюючи математичну модель.

У пристрої біометричної ідентифікації SpeedFace, що є важливою частиною системи розпізнавання Face ID, використовуються новітні технології розпізнавання осіб [3]:

1) Visible Light - дозволяє швидко ідентифікувати користувача за обличчям без його повної зупинки перед терміналом;

2) безконтактне розпізнавання по долоні, за новим алгоритмом ZKPalm, що поєднує 3 технології воєдино:

- розпізнавання форми долоні Palm Shape,
- розпізнавання відбитка долоні Palm Print
- та розпізнавання кровоносних судин Palm Vein.

Face ID вважається одним із найбезпечніших методів біометричної автентифікації, завдяки стереозйомці, дві камери краще розпізнають глибину сцени чим підвищують точність даних в кілька разів:

– захист від спуфінгу – завдяки використанню 3D-карти обличчя та інфрачервоних датчиків, систему неможливо обдурити за допомогою звичайної фотографії або 2D-маски;

– конфіденційність даних – зашифрована біометрична інформація зберігається виключно на пристрої, в захищеному процесорі, ніколи не передається на сервер або в хмару.

Структурну схему такої системи контролю доступу можна представити у такому вигляді (рис. 1.2) [3].

Рисунок 1.2 – Структурна схема системи контролю доступу з пристроєм безконтактної біометричної ідентифікації по лицю та долоні

Пристрій безконтактної ідентифікації по обличчю та по долоні SpeedFace RFID , що здійснює безпосередньо контроль доступу в такій системі показано на рисунку 1.3 [3].

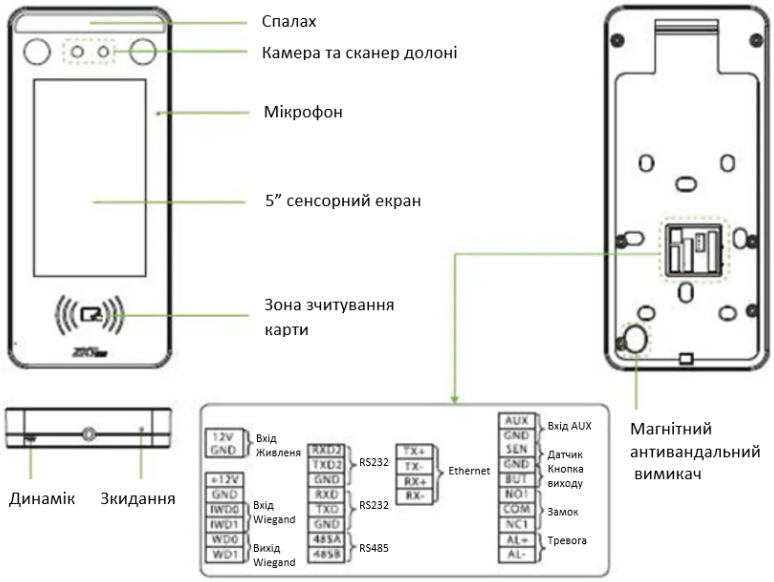


Рисунок 1.3 – Пристрій безконтактної ідентифікації по обличчю та по долоні SpeedFace RFID

1.3 Системи доступу за відбитками пальців на нейромережах

Системи доступу за відбитками пальців на нейромережах – це сучасні біометричні СКД, які використовують штучний інтелект та машинне навчання для високоточного розпізнавання унікальних візерунків пальців, забезпечуючи надійніший захист, швидкість та зручність, на відміну від класичних методів, інтегруючись у процеси обліку робочого часу працівників та відеоспостереження, що робить їх прогресивним рішенням для контролю доступу. Загальний принцип роботи такої системи доступу за відбитками пальців на нейромережах [5]:

1) зчитування відбитку. Сенсор зчитує папілярний візерунок пальця, створюючи його цифрове зображення;

2) обробка нейромережею зображення відбитку. Алгоритми машинного навчання аналізують отримані дані, виділяючи ключові точки (мінуції) та створюючи унікальний шаблон (біометричний шаблон), який не є самим зображенням, а є математичним кодом ;

3) порівняння. Отриманий шаблон відбитку порівнюється з шаблонами, що зберігаються в базі даних системи;

4) прийняття рішення. Якщо відбувається збіг зі заданим рівнем точності, система дозволяє доступ (розблоковує замок), фіксує подію (жрнал).

Перевагами такої системи є

– висока надійність, НМ покращують точність ідентифікації, зменшують помилки при прийнятті рішень;

– швидкість, миттєве розпізнавання та рішення про доступ;

– безпека, неможливість підробки відбитків, на відміну від карт або паролю, дані зберігаються у вигляді коду;

– інтеграція, можливе поєднання з відеокамерами для розпізнавання обличчя різними сканерами і функціями (вимір температури, тощо);

– зручність, не потрібно носити карти, пам'ятати паролі.

1.4 Деякі небажані підходи для ідентифікації за обличчям та відбитком пальців

Ми розглянули системи ідентифікації за обличчям та відбитками пальців. Але вчені з Америки вже створили штучну систему з алгоритмом DeepMasterPrint, що самостійно створює відбитки пальців, які є універсальними і можуть підійти як фрагмент для відбитку живої людини, і кількість такого співпадіння не є поодинокою [2]. Під час розробки такого алгоритму було використано генеративно-змагальну нейромережу, яка навчена на особистих даних з біометрії людей, кількість яких дорівнює 5400. Вчені за мету ставили показати деяким розробникам систем, що у якості

способу ідентифікації використовують лише частину зображення відбитку, що така практика не зовсім безпечна, хоча і знижує витрати часу на розпізнавання.

Так Філіп Бонтрейджера з Нью-Йорку з колегами запропонували алгоритм автоматичної генерації універсального зображення відбитків пальців – система Deep MasterPrints (рис. 1.4).

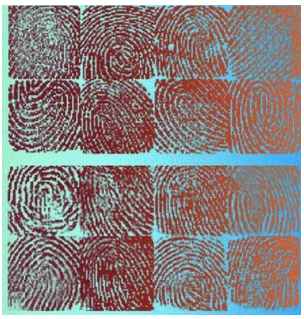


Рисунок 1.4 – Зображення універсальних відбитків пальців

Після того як створення зображення відбитків склалося успішно, такий алгоритм починає шукати використані генератором змінні, в такий спосіб підбирається універсальний відбиток, що буде підходити для більшої кількості відбитків з вибірки, що представлена для навчання. Зображення , що створено у такий спосіб є ефективнішим в десять раз від відбитка що створюється у випадковий спосіб.

Цю систему на даний час використовують як тренувальну під час пошуку покращення алгоритмів розпізнавання за біометричними характеристиками відбитків пальців.

Отже зробивши аналіз систем ідентифікації для систем доступу можна виділити основні принципи за яким працюють такі системи – бажаною є безконтактна технологія розпізнавання долонь для гігієнічної ідентифікації осіб, та верифікація по відбитку пальця , що поєднали в собі новітні технології розпізнавання.

1.5 Технології для розпізнавання відбитків пальців

Для біометричної ідентифікації є багато технологій розпізнавання відбитків пальців, що базуються на різних підходах та методах. Розглянемо деякі з них. Сканери відбитків пальців, їх три основні типи: ємнісні, оптичні та ультразвукові. Різняться вони за методом отримання зображення відбитка пальця [6].

Оптичне розпізнавання відбитків пальців є найбільш використовуваним, спирається на світло та оптику у вигляді світлочутливої матриці для отримання зображень із високою роздільною здатністю. Принцип дії оптичного методу показано на рисунку 1.5.

Перевагою є можливість монтажу такого датчика в екран без додаткових датчиків. Недоліком є те, що вони менш точні за умов низької освітленості.

Ультразвукове розпізнавання відбитків пальців [6,10] схоже на ультразвукове діагностування: ультразвукові хвилі, що генеруються за допомогою електричного струму, проходять через захисне скло смартфона, зустрічають відбиток пальця, відбиваються від його заглиблень і виступів, повертаються до сканера і перетворюються на цифровий сигнал (рис. 1.6).

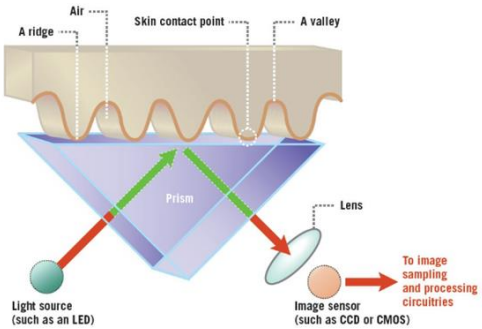
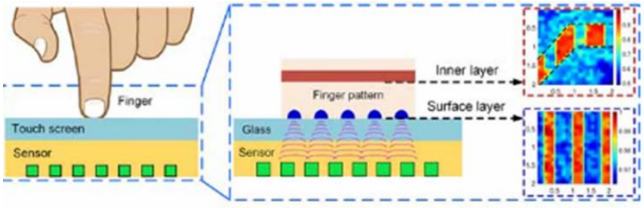


Рисунок 1.5 – Принцип дії оптичного методу



Рисунок– 1.6 Ультразвукове розпізнавання відбитків пальців

Забезпечує більш безпечне та точне зчитування порівняно з оптичними методами, використовують для розблокування смартфона. Ультразвуковий датчик є високоточним, оскільки аналізує глибину шкірного покриву, а не лише поверхню, більш чутливий навіть з вологими або брудними пальцями, його складніше обійти, оскільки використовується складніші методи зчитування у порівнянні з оптичним.

Ємнісне розпізнавання відбитків пальців, що спирається технологію датчиків для вимірювання зміни електричної ємності між виступами та западинами папілярного візерунка пальця для створення цифрового образу відбитку для автентифікації [6,10]. Коли є контакт з датчиком, кожен піксель сканера визначає зміни в електричному полі, із-за шорхостей відбитка пальця. Переваги – ємнісні датчики дуже точні, оскільки вони створюють електричний знімок відбитка, важко підробити, швидкість зчитування відбитку долі секунд, вони найменш чутливі до бруду та вологи.

Існують також теплове розпізнавання через термодатчики, методом натискання, метод поверхневих хвиль і багатоспектральне розпізнавання (рис. 1.7) [6].

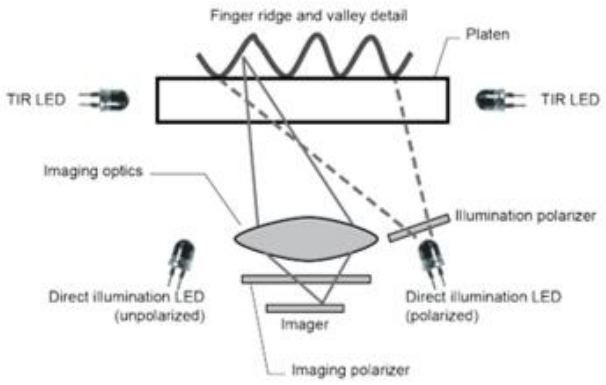


Рисунок 1.7 – Багатоспектральний аналіз з датчиками типу MSI

Для розпізнавання відбитків пальців на основі систем штучного інтелекту використовуються алгоритми машинного навчання . Системи розпізнавання у реальному часі керуються технологіями, що допомагають відрізняти живі пальці людини від штучно зробленого відбитку .

Отже цифрові зображення відбитків пальців можливо отримати з різних типів датчиків, що розглянуто вище, з них найбільш розповсюдженими для такого завдання є оптичні датчикі.

2 АНАЛІЗ АКТУАЛЬНИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Ознаки за якими можна ідентифікувати особу пов’язані, як правило, з її фізіологічними особливостями, і дозволяють її однозначно виділити серед інших. Такі ознаки як: геометрія побудови руки або форма кісті, відбитки пальців, складний особливій візерунок сітківки ока, або особливості його райдужної оболонки, графічний портрет. Все це складає інфрачервону карту людини. Також є характеристики і особливості рукописного відбитку-почерку, мови, а також клавіатурний або комп’ютерний почерк та інші фізіологічні особливості роблять людину особливою , лише одна двадцяти чотирьох мільйонна доля є того що чиїсь відбитки пальців співпадають з відбитками іншої людини, тобто практично дорівнює нулю.

Виділяють основні дві категорії методів порівняння відбитків: співставленння цілого рисунку відбитка або порівняння визначених точок на ньому [7]. Метод шаблонної ідентифікації порівнює два зображення, і дозволяє побачити їх схожість або несхожість. В такий спосіб знаходять дублікати відбитків в системах зчитування відбитків.

Метод кореляційного порівняння використовує по-піксельне порівняння двох відбитків пальців, приналежність одного з низ відома. При такому методі враховуються спотворення зображення та різні шумові ефекти. Технологію , що частіше обирають для розпізнавання, є порівняння визначних точок.

А методом, що частіше за інші використовують для біометрії є розпізнавання за відбитком. Він є зручним для використання , тому що у кожної людини присутні різні папілярні візерунки пальців, і для людини протягом життя вони остаються незмінними. Зібравши дані за допомогою сканеру, занести в систему ідентифікації отримують можливість в криміналістиці або прикордонній службі мати свою базу для швидкої

ідентифікації. Такі системи безпечні за рахунок технологій перетворення зображення у цифровий код та шифрування [7].

Розпізнавання по сітківці ока. Відбувається завдяки малюнку кровоносних судин в оці, для відображення малюнка необхідно подивитися на світлодатчик, що просканує рисунок судин очей спеціальною камерою.

Розпізнавання за райдужною оболонкою ока. Працює через особливості райдужної оболонки. Спеціальна камера повинна просканувати очі і побудувати необхідний код для надання доступу.

Розпізнавання за формою долоні. Здійснюється по геометричній формі кисті рук, сканер отримує тривимірний знімок руки і перетворює його в код для обробки та ідентифікації.

Розпізнавання за формою обличчя за рахунок побудови двох чи тривимірних образів обличчя, із допомогою камери відображаються частини обличчя та вирисовуються контури його, з подальшим використанням для ідентифікації людини.

В методах біометричної ідентифікації можна виділити дві групи:

– статичні методи, використовують фізіологічні характеристики людини;

– динамічні методи використовують особливості поведінки людей, це можуть бути будь-які підсвідомі рухи під час ходьби або виконанні конкретних дій.

Статичні і динамічні методи біометричної ідентифікації є взаємопов’язаними між собою і взаємодоповнюючими один одного напрямами. Перевагами статичних методів ідентифікації є їх відносно стійка незалежність від психічного стану користувача системи ідентифікації, і можливість створення умов для використання швидкої ідентифікації потоку людей або великої групи їх. [10]. Біометрична ідентифікація на динамічних характеристиках здійснюється у простіший спосіб, бо не потребує дорогого обладнання, а час її проведення обмежується використанням програмного забезпечення, за мінімальної підтримки фахівця в експлуатації такої системи

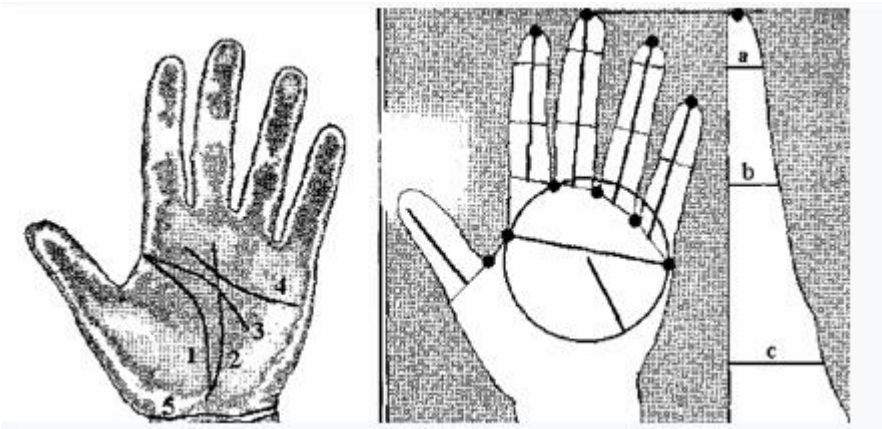
з використанням ПЗ динамічної ідентифікації. Нижче наведено, у вигляді таблиці для зручності порівняння, узагальнення основних статистичних біометричних характеристик із видами їх реалізації (Рис 2.1) [10].

Біометрична характеристика	Реєструючий пристрій	Зразок характеристики	Риси характеристики для досліду
Геометрична будова руки	Запатентований пристрій	Тривимірне зображення: зверху/з обох боків	Висота, ширина кісток суглобів кісті і пальців
Відбиток пальця	Периферійний пристрій, ПК, карта стандарту PC-card, маніпулятор миша, мікросхема або вбудований пристрій зчитування	Зображення відбитку пальців: оптичне, на кремнієвому фотоприймачі, ультразвукове-безконтактне	Розташування і напрям гребінчастих виступів і роздвоєнь на відбитку, дрібні деталі
Особливості рисунку сітківки ока	Запатентований настінний або настільний пристрій	Зображення сітківки	Розташування кровоносних судин на сітківці
Райдужна оболонка ока	Відеокамера інфрачервоного діапазону, камера для ПК	Чорно-біле зображення райдужної оболонки ока	Смужки і бороздки на райдужній оболонці ока
Портрет обличчя	Відеокамера, камера для ПК, фотоапарат	Зображення особи оптичне або теплове	Відносне розташування і форма рота, носа скули, брови ін.

Рисунок 2.1 Основні статистичні біометричні характеристик та їх реалізації

2.1 Метод розпізнавання за формою руки

Статичний метод ідентифікації за формою руки базується на аналізі геометричних параметрів форми кісті людини, що є особливою для кожного. Для реалізації цього методу застосовуються спеціалізовані технічні засоби, які забезпечують отримання тривимірного зображення кисті руки. Отримані дані використовуються для формування унікального біометричного шаблону, що забезпечує однозначну ідентифікацію особи. В межах даного методу виокремлюють два основні підходи: перший передбачає використання виключно геометричних характеристик кисті руки, тоді як другий додатково враховує образні характеристики, зокрема структуру з’єднань між фалангами пальців та візерунки кровоносних судин. (рис. 2.2).



а) б)

а) візерунок на долоні,

б) набір контрольних точок та сукупність із 17 геометричних характеристик кисті руки

Рисунок 2.2 – Вигляд рисунку судин долоні та особливості фаланг пальців

На рисунку 2.2 бачимо лінії, що складають карту судин із п’яти ліній на долоні (а), а також систему контрольних точок і сімнадцять геометричних

ознак кисті руки (б). До основних геометричних ознак належать: параметри ширини долоні, коло з радіусом, що вписується в долонь , для пальців їх ширина і довжина, для кісті вимірюють у трьох точках висоту . потім всі ці ознаки складаються в так званий єдиний вектор значень [10].

Ідентифікація за методом на основі вектора ознак є відносно простим у реалізації. На початковому етапі здійснюється зняття кількох проекцій кисті руки користувача, для кожної з яких формується окремий вектор значень. На основі множини таких векторів створюється спеціальний клас, у межах якого всі ознаки усереднюються, після чого формується еталонний образ, що відповідає центру класу. Якщо таке порівняння образу з еталоном відбулося успішно, то його буде додано в клас ознак виходу.

Порівняння двох образів може здійснюватися за різними критеріями, найпоширенішим з яких є мінімальна відстань між досліджуваним образом та еталоном. Більш складні методи передбачають аналіз чотирьох характеристик, три з яких є характерними геометричними розмірами, а четверта — півтоновим зображенням складок шкіри в місцях згину між фалангами пальців. Такий підхід дозволяє зменшити похибки сканувального обладнання, проте характеризується високою вартістю реалізації через складність використовуваних сканувальних пристроїв.

2.2 Метод біометричної ідентифікації на основі відбитків пальців

На зображенні відбитка пальця, отриманому за допомогою сканера, залежно від його якості, можуть бути виділені характерні ознаки, які в подальшому використовуються для цілей біометричної ідентифікації. На базовому технічному рівні, зокрема за умови роздільної здатності зображення в межах 300–500 dpi, на поверхні відбитка можливо виділити значну кількість невеликих деталей, за якими здійснюється класифікація. Водночас у більшості систем ідентифікації використовуються лише два основні типи особливих точок візерунку, що складають картину папілярних ліній:

– кінцеві точки , такі у яких чітко видно, що папілярні лінії завершуються;

– точки роздвоєння, такі у яких папілярні лінії розділяються на дві лінії.

За умови отримання чіткого зображення, роздільна здатність якого складає 1000dpi, стає можливим отримання зображення потових залоз, які є дрібними деталями у структурі папілярних судин (рисунок 2.3). На відповідному зображенні пори позначаються порожніми колами, тоді як кінцеві точки та точки розгалуження - суцільними чорними колами. Просторове розташування зазначених елементів може бути використане для ідентифікації особи. Проте такий підхід має обмежене практичне застосування через складність отримання зображень необхідної якості поза лабораторними умовами.

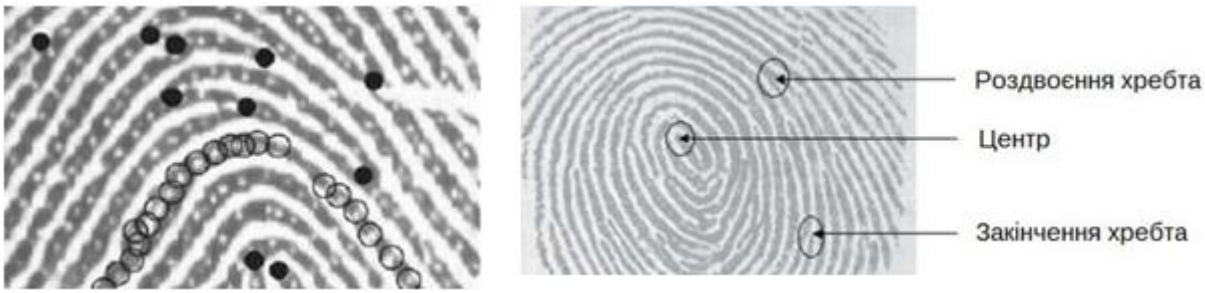


Рисунок 2.3 – Зображення папілярного візерунка з ідентифікованими порами та точками роздвоєння

2.3 Методи і техніки розпізнавання цифрових відбитків пальців

Автоматизація розпізнавання відбитків пальців дозволяє уникнути значної кількості проблем, що виникають при ручній обробці Електронні безфарбові сканери забезпечують отримання зображень папілярного візерунка пальця з достатньою якістю, що є критерієм для вибору алгоритму формування біометричної згортки відбитка пальця. Для того щоб отримати цифрове зображення відбитків пальців використовують різні типи датчиків. А

саме оптичні, ультразвукові, ємнісні і теплові, причому оптичні датчики наразі є найбільш поширеними.

Раніше було відмічено, що з двох методик порівняння відбитків при розпізнаванні найбільш використовуваною є методика, що базується на деталях відбитка, вона є найпоширенішою: папілярні візерунки пальців зчитуються за допомогою сканера та зберігаються у цифровому коді.

Система ідентифікації за деталями відбитка включає три основні етапи:

– попередня обробка зображень;
– виділення ознак;
– зіставлення отриманих ознак.

Існують методики для відновлення ознак відбитка з інформації про деталі. Один із підходів передбачає використання шаблону відбитка пальців, де деталі представлені за допомогою спіральних кривих, що відображають структуру сусідства деталей і трикутників Делоне низького порядку.

Симетричний метод хешування деталей відбитків пальців, зберігаючи розміщення деталей за схемою одностороннього перетворення геометричної конфігурації точок в код, що євектором із фіксованою довжиною, забезпечує захист відбитка-оригінала,

Обробка самого відбитка виконується за алгоритмом SIFT, а вектори ознак фіксованої довжини використовуються для представлення набору спектральних деталей зображення.

Метод зіставлення відбитків, спирається на оцінювання западини та гребні папілярних ліній. Він застосовується для пошуку пар контрольних точок зображення, що будуть розглядатися надалі для розгляду. Для кожної пари здійснюється зіставлення гребнів, після чого поступово узгоджуються всі контрольні точки та гребні за ієрархічною системою відповідності, що використовує ознаки на трьох рівнях:

1) загальний візерунок;

2) дрібні точки;

3) пори та контури гребнів.

Інший метод без попереднього вирівнювання ознак полягає у використанні триплетів деталей про геометричну інформацію відбитків для відтворення її у шаблоні. Метод спосіб опису кожної контрольної точки функцією обертання, яка обчислюються на основі орієнтації локальної області навколо контрольних точок. Отримане інваріантне значення використовується у двох змінних функціях для визначення поступального та обертального рухів деталей у шаблоні, який можна зберігати та за потреби скасовувати [11].

Для усунення проблеми оптимального збігу між двоточковими шаблонами при геометричних трансформаціях застосовують узгодження точкового шаблону із шаблоном помилкових точок. Співставлення шаблонів здійснюється на основі локальної структури деталей шаблонів

Ідентифікація користувача виконується шляхом порівняння оцінки відповідності з встановленими пороговими значеннями.

Впроваджуються також онлайн-системи верифікації відбитків пальців, які працюють у два етапи: спершу вилучаються деталі з вхідного зображення, а потім виконується їх зіставлення з відповідним шаблоном за алгоритмом еластичного зіставлення на основі вирівнювання.

Особливу увагу приділяють методам збереження шаблонів зображень відбитків пальців. Поняття «захист шаблонів» є збірним терміном, що охоплює різні підходи до забезпечення конфіденційності та безпеки біометричних даних [9]. Такий підхід, орієнтований на трансформації та біометричні криптосистеми, можна подати у вигляді схематичного зображення (рис. 2.4).

Функції трансформації можуть модифікувати біометричні дані таким чином, що відновлення вихідних даних із трансформованих шаблонів стає неможливим. Біометричні криптосистеми можуть бути інтегровані безпосередньо або використовуватися для генерації секретів на основі біометричних даних. Одним із рішень є застосування шаблону зі змішаним ключем, який комбінує шаблон користувача із секретним ключем для формування нової форми шаблону. Такий біометричний алгоритм

шифрування, що дозволяє отримувати цифрові ключі, забезпечує безпечне керування криптографічними ключами [11, 12].

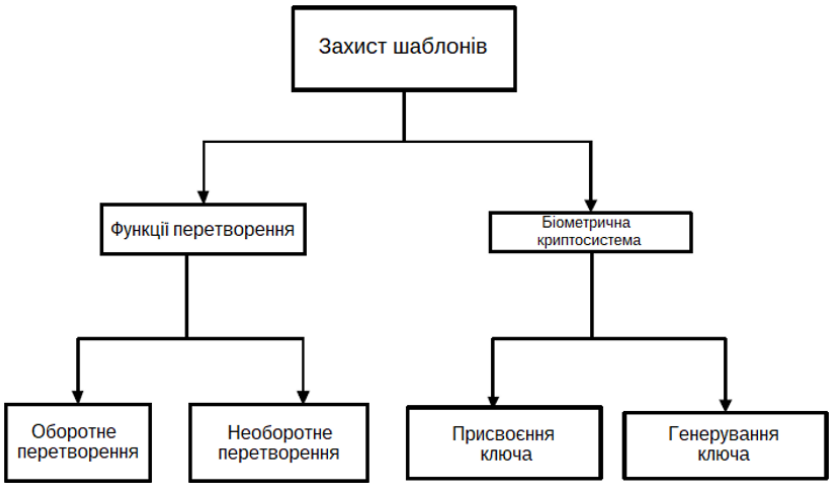


Рисунок 2.4 – Класифікація методів захисту збереження шаблонів.

Розробляються стандарти методів зберігання біометричних даних, які забезпечують відновлюваність зображень відбитків пальців, відповідають вимогам безпеки шаблонів і передбачають різні підходи та розробку схем для захисту шаблонів на рівні деталей (табл.2.1).

Таблиця 2.1 – Різні методи трансформації функцій для захисту шаблонів.

Метод трансформації функцій	Особливості зображення	Представлення, що є результатом
Деталі спектру	З виділенням деталей	Результат є вектором
Шифрування біометричних даних зображення	Рисунок відбитку пальця	Результат є ветором
Показчик деталей	Специфічні деталі	Результат є вектором
Потрійна гістограма деталей	Трійки деталей	Результат є вектором
Прямокутна Агрегація	Групування деталей	Вектор зв’язку
Симетричний хеш	Хеш деталі	Хеш функції
Дрібні структури	Дрібні деталі	Дрібні деталі

2.4 Інші методи ідентифікації особи

Існують також інші біометричні технології, що базуються на фізіологічних характеристиках людини, зокрема:

– порівняння ДНК, на сьогодні є найбільш точним біометричним методом, що дозволяє однозначно ідентифікувати особу, за винятком однояйцевих близнят, які мають однаковий генотип. Біометричні системи на основі ДНК забезпечують пряме підтвердження ідентичності;

– відбиток долоні , система ідентифікації використовує розташування ліній на долоні людини і функціонує аналогічно до технології розпізнавання за відбитками пальців;

– судинні рисунки, базуються на унікальному розташуванні вен у різних частинах тіла, зокрема на зап’ястях та тильній стороні долоні;

– біодинамічні сигнали включають: серцеві імпульсні сигнали; імпульси нейронів мозку, що є одночасно і потенціалом до дії і електричним сигналом для систем діагностування; сигнали діяльності легенів.

Для ідентифікації особи датчиком «біодинамічного підпису» достатньо знаходження людини у контакті з датчиком 8 секунд, за цей час датчик обробляє сигнали та виконує ідентифікацію особистих індивідуальних параметрів людини. Ідентифікація методом райдужної оболонки ока спирається на виділення частотної інформації про саму структуру оболонки і збереження її у коді «iriscode» , райдужний , що використовується системою Даугмана і зберігається у БД.

Отримання райдужного коду за три кроки :

– вилучення зображення райдужної оболонки із отриманого камерою загального зображення ока;

– обробка методами усунення світлових завад, або шуму

– обробка зобраотриманого зображення, наприклад, усунення шуму (denoising), поліпшення зображення (enhansing) за рахунок вирівнювання гістограми, корегування блиску, здійснюється перехід до прямокутного

зображення в декартову систему координат. Частина зображення може бути відсіченою щоб уникнути зайвих помилок;

– опис зображення кодом після операції фільтрації.

Готовий код записаний у бітовій послідовності, обирається критерій порівняння, що буде кодом Хемінга, що використовується в системах Даугмана, Тіссе [12], що дозволить визначити всі помилки, але не стане їх виправляти.

Методи в більшості своїй працюють із зображеннями у градаціях сірого кольору або із картами яскравості зображення, у даному випадку кольорова складова є надлишковою тому працюють з чорно білим зображенням.

Ідентифікація за зображенням обличчя є статичним методом ідентифікації, що передбачає побудову двовимірного або тривимірного образу з обличчя людини. Спеціальне ПЗ на зображенні, зробленому камерою та на однім або на кількох одразу, різних зображеннях виділяє контури брів, очей, носа, губ та інших характерних ознак. Додатково обчислюються відстані між цими точками та інші параметри, які залежать від конкретного алгоритму, що застосовується для ідентифікації.

Ідентифікація особи за голосом використовує наявну телефонну мережу та стандартні звукові карти сучасних ПК. Основним недоліком систем розпізнавання за голосом є те, що саму парольну фразу складно довго зберігати у секреті. Сучасні акустичні засоби дозволяють здійснювати прослуховування з копіюванням парольної фрази, у з’вязку з чим, голосові системи важливо комбінувати з технологіями захисту для біометричної ідентифікації. Помилки в роботі тахих систем складають всього 1-2%.

Для ідентифікації абонента за голосом необхідно мати мовний шаблон, з яким порівнюється голосовий ключ, введений у систему [10]. Для спрощення аналізу мовний сигнал попередньо піддають дискретизації з використанням частотного або вейвлет-перетворення. Ідентифікація абонента може виконуватися за такими показчиками :

– короткочасна енергія сигналу визначається функцією короткочасної енергії з використанням вікон Хеммінга;

– автокореляційна функція дозволяє визначити енергію та періодичні властивості сигналу;

– число переходів сигналу через нуль, що означає високі частоти відповідають великій кількості переходів через нуль, низькі – меншій кількості переходів;

– спектр сигналу;

– коефіцієнти лінійного передбачення;

– кепстральні коефіцієнти.

Окрім голосової біометрії, існують методи ідентифікації за динамікою рукописного підпису користувача (факсимільний підпис), за клавіатурним почерком (наприклад, під час введення пароля) та за почерком миші [9, 10].

Основні динамічні біометричні характеристики людини, а також варіанти їх реалізації наведено в таблиці 2.2.

Таблиця 2.2 Основні динамічні біометричні характеристики ідентифікації, та види їх реалізації.

Характеристика	Рєєструючий пристрій	Зразок шаблону для порівняння	Риси, що досліджуються
Голос	Мікрофон телефон	Запис голосу і значення його динамічних вимірів	Тривалість запису образу голоса, частота , модуляція
Підпис	планшет для підпису, перо для підпису	Зображення підпису	Швидкість прописування, порядок ліній, тиск та загальний вигляд підпису

Продовження таблиці 2.2

Характеристика	Рєєструючий пристрій	Зразок шаблону для порівняння	Риси, що досліджуються
Динаміка натискань клавіш	Клавіатура	Ритм машинопису	Час затримки, протягом якого утримується конкретна клавіша, Час «польоту», що потрібен для переходу з одної клавіши на іншу
Динаміка роботи з «мишею»	маніпулятор «миша»	Образ характерної траєкторії	Характерні точки траєкторії , інші параметри траекторії

Ідентифікація за почерком миші під час роботи користувача в системі демонструє надійність розпізнавання на рівні 0,8–0,9 [5].

Для цього екран розбивається на зони, в яких курсор миші перебуває найчастіше, а характеристики руху миші між зонами аналізуються кожні дві хвилини [11].

Аналіз почерку миші може виконуватися повністю або шляхом обробки окремих сегментів після попередньої сегментації зображення почерку (табл. 2.3) [8, 9].

Розвиваються нові технології біометричної ідентифікації , останніми є аналіз форми вушної раковини, де за допомогою Web-камери отримуються зразки для порівняння, система «електронний ніс» для розпізнавання за запахом тіла і технологія спектроскопії шкіри людини.

Таблиця 2.3 – Порівняльний аналіз методів ідентифікації користувача за динамікою рухів маніпулятора «миші»

Метод	Порівнювані характеристики або алгоритм-рішення	Розмір бази даних, ймовірність помилок
Порівняння рядків	Глобальні характеристики Сполучені рядки	20–103 користувачів, 10 – 30 підписів кожного. Ймовірність помилки 3–5%
Ланцюги Маркова	Алгоритм Баума-Велша Алгоритм Вітербі	14–15 користувачів, 20–30 підписів від кожного. Ймовірність помилки 1–4%
Нейронна мережа	Багатошаровий персептрон	27 користувачів, 30 підписів від кожного. Ймовірність помилки 4%
Байєсівська мережа	Метод головних компонентів	27 користувачів, 30 підписів від кожного. Ймовірність помилки 0,5–4%

3 ДОСЛІДЖЕННЯ СУЧАСНИХ НЕЙРОМЕРЕЖ З БАГАТОШАРОВОЮ СТРУКТУРОЮ

Будь-яка структура штучних нейронних мереж (ШНМ) складається з:

– нейронів, що є базовою обчислювальною одиницею, саме вони приймають вхідні дані, виконують обчислення та передають вихідні значення іншим нейронам. Кожен нейрон має зв’язки з іншими нейронами та ваги, що визначають важливість вхідних даних.

– шарів. Нейрони організовані в шари. Зовнішні дані отримує вхідний шар, приховані шари виконують проміжні обчислення і вихідний шар надає результуючі дані. Отже нейронна мережа складається з одного або декількох шарів, залежно від складності завдання;

– ваги. Кожний зв’язок між нейронами має вагу, що є визначенням важливості вхідного сигналу для кожного нейрона в мережі. Саме ваги є ключовими параметрами для налаштування її поведінки, вони навчаються під час навчання мережі;

– функцій активації, що додають нелінійність в роботу нейронів, це дозволяє мережі виявляти складні закономірності даних. Від функції активації залежить яким буде вихід нейрона на основі вхідних даних та ваг.

Структура штучних нейронних мереж (ШНМ) складається з штучних нейронів, що представляють собою елементи обробки. Вона має організацію у вигляді трьох взаємопов'язаних шарів: вхідного, що може включати один або кілька шарів, прихованого та вихідного (рис. 3.1).

Багатошарові мережі утворюватися каскадами шарів. Вихід одного шару є входом наступного. Якщо активаційна функція між шарами буде нелінійною то БШМ вимагають збільшення обчислювальної потужності. Обчислення виходу шару полягає в множенні вхідного вектора на першу вагову матрицю з подальшим множенням (за відсутності нелінійної активаційної функції) результуючого вектора на другу вагову матрицю.

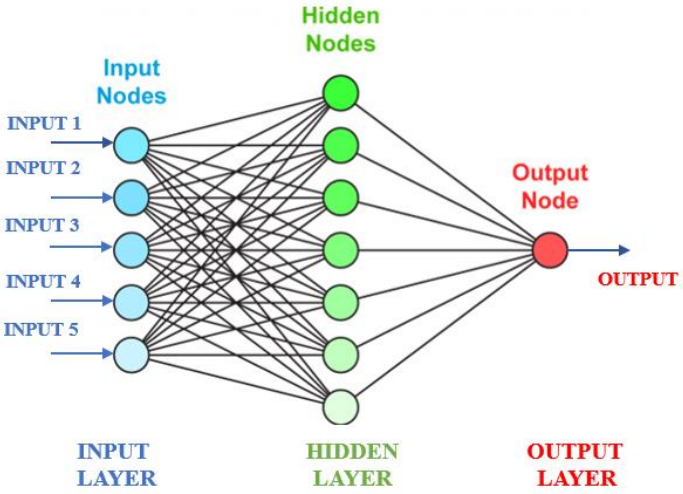


Рисунок 3.1 – Структура ШНМ у вигляді 3-х взаємопов'язаних шарів

Отже, будь-яка багатошарова лінійна мережа може бути представлена як сума еквівалентних одношарових мереж (рис. 3.2)

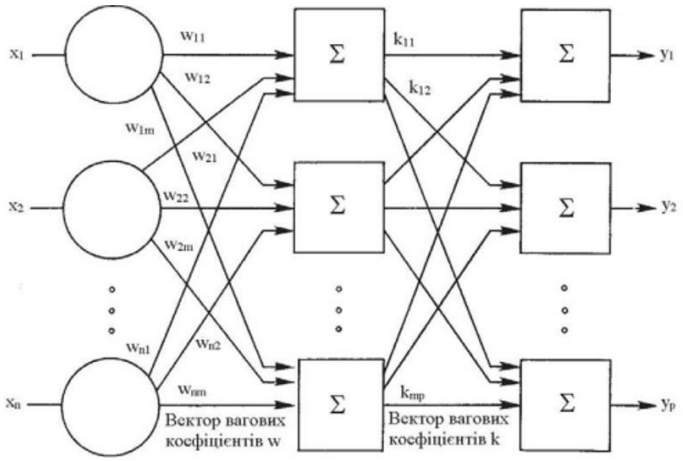


Рисунок 3.2 – Структура лінійної ШНМ у вигляді суми одношарових мереж

Вхідний шар НМ складається з нейронів, що мають передавати інформацію в приховані шари. Прихований шар , у свою чергу, передає отриману інформацію у вихідний шар. Кожен з нейронів включає: входи з вагами, що представляють собою синапси, функцію активації, визначають вихідну інформацію в залежності від заданого входу, і один вихід. Синапси є регульованими параметрами, що перетворюють нейронну систему мережі в

параметризовану систему. Принцип роботи нейромережі в тому, щоб передача даних від вхідного шару до вихідного проходила через шари нейронів з оновленням ваг і застосуванням функції активації.

Мережа навчається, пристосовується до нових даних і стає здатною до виконання різноманітних завдань з класифікації, обробки зображення, регресії Машинне навчання нейромережі дозволило автоматизувати такі складні завдання , які раніше було важко вирішувати. Здатність навчатися нейронної мережі обумовлена налаштуваннями, вбудованими в її структуру, ми можемо спостерігати розвиток нейромережі на всіх етапах та вносити коригування в її розвиток за потребою.

3.1 Багатошаровий персептрон

Багатошаровий персептрон (MultilayerPerceptron, MLP) є типом штучного нейронного шару, який складається з кількох шарів нейронів, включаючи вхідний, приховані та вихідний (рис.3.3) [13].

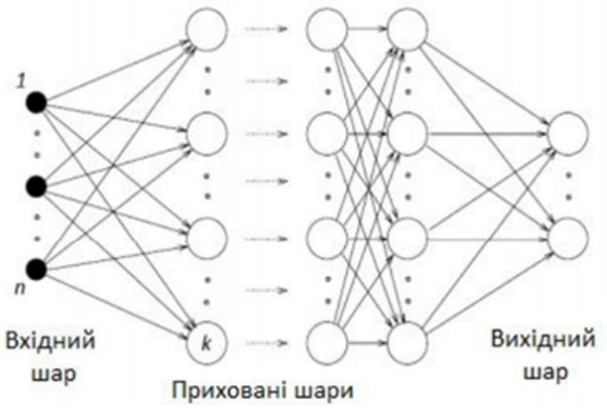


Рисунок 3.3 – Багатошаровий персептрон

Основна його особливість –один прихований шар робить його більш гнучким та здатним до вивчення складних нелінійних залежностей в даних. Вхідний шар має кількість нейронів рівну кількості вхідних ознак у вхідних даних. Кожен нейрон це вхідна ознака. Приховані шари обчислюють і вивчають залежності між вхідним та вихідним шарами. Вихідний шар генерує

вихід моделі. Багатошаровий персептрон призначений для завдань класифікації та регресії для машинного навчання за методами оптимізації ваги для мінімізації помилок передбачення. Як що порівняти з ANN, то в MLP нейрони повністю з’єднані з нейронами в наступному шарі, а в ANN можуть бути частково з’єднані, повністю з’єднані або мати цикли. MLP добре працюють на обробці сигналів та розпізнаванні зображень [13, 14].

3.2 Неглибокі нейронні мережі

Це нейронні мережі з невеликою кількістю шарів, можуть мати лише один або кілька прихованих шарів. Основні характеристики неглибоких нейронних мереж є мінімальна кількість шарів, обмежена абстракція, що дозволяє швидше тренування, що важливо для невеликих задач.

3.3 Рекурентна нейронна мережа

Рекурентна нейронна мережа (RNN) має такий тип штучного нейронного шару, здатний використовувати внутрішню пам'ять для обробки часових рядів, мовлення або тексту. Головною особливістю її є наявність зв'язків між нейронами для формування напрямлених циклів у графі обчислень,. нейронні шари передають інформацію з попередніх моментів часу (рис. 3.4). Нейрони та ваги в RNN визначають силу зв'язків між нейронами, петлі на кожному шарі в архітектурі дозволяють моделі отримувати інформацію від попередніх шарів і від свого рекурентного зв’язку.

Розрізняють модефікації рекурентної нейроннох мережі [16]:

1) BRNN (bidirectional recurrent neural network) – э двонаправлена рекуррентна нейронна мережа, в якій є два приховані шари з однаковим входом з’єднані у протилежних напрямках. Вихідний шар RNN з минулих та майбутніх станів отримує інформацію одночасно. За принципом архітектури

BRNN працює так Принцип архітектури BRNN в тому, щоб розбити нейрони звичайної RNN на два напрямки:

– один для напрямку доданого часу;

– другий для від’ємного часу;

2) GRUs – форма архітектури рекурентних нейронних мереж, що обробляє послідовні дані –текст або часові ряди, за допомогою спеціалізованих механізмів керування;

3) LSTM – довга короткочасна пам’ять – long short-term memory, така мережа вміло розв’язує проблеми зниклого градієнта стабілізує роботу з послідовностями протягом тривалого періоду, клітинний стан є особливістю такої мережідля здійснення вибору: що пам’ятати або забути із попередніх кроків завдання.

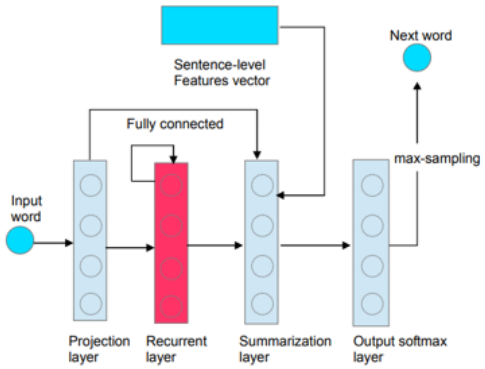


Рисунок 3.4 – Модель RNN

3.4 Згорткова нейронна мережа

Таку мережу використовують для розпізнавання за відбитками пальців або образами обличчя, завдань пов'язаних з розпізнаванням патернів, що розпізнають тривимірні об'єкти, [11]. Робота згорткової нейронної мережі базується на фільтрах (визначниках ознак) та картах ознак. Фільтр представляє собою матрицю, яка виділяє конкретну ознаку на вихідному зображенні, визначення базується на операції згортки фільтром оригінального зображення. Результати згортки, що визначають місцезнаходження ознак у вихідному

зображенні називають карта ознак. Ідею згорткового шару така, що кожен вихідний нейрон з’єднано лише з обмеженою областю вхідної матриці

Недоліком згорткових нейронних мереж є складність архітектури.

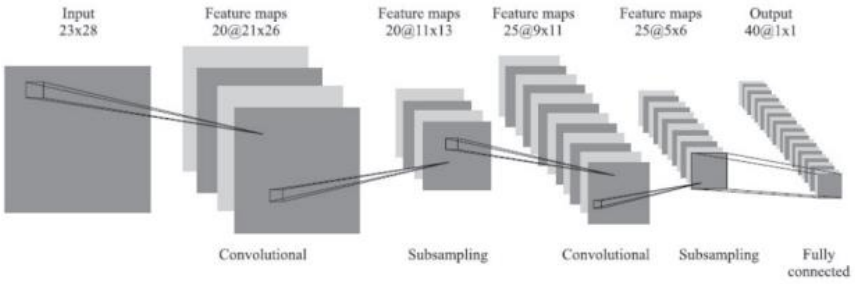
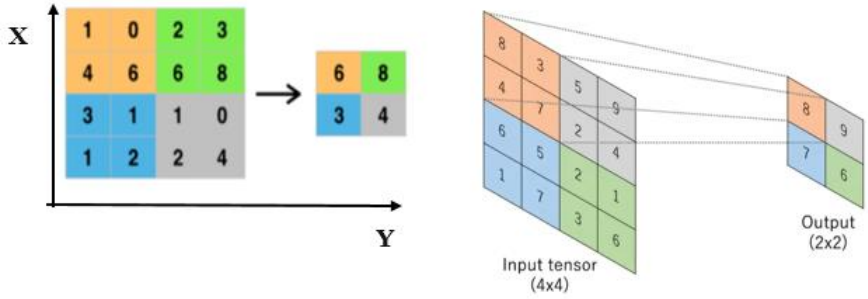


Рисунок 3.5 – Архітектура згорткової мережі CNN

CNN є проміжний варіант між біологічними мережами та звичайним багатошаровим персептроном і на сьогоднішній день досягають найкращих результатів у обробці зображень відбитків, точність їх розпізнавання перевищує звичайні нейронні мережі на 15%. Згорткові мережі є ключовою технологією глибокого навчання [12].

Незважаючи на великий розмір, ці мережі мають обмежену кількість змінних параметрів. Матриця ваг графічно кодує будь-яку ознаку, із-за своєї побудови, де кожен шар, отриманий внаслідок операції згортки з відповідною матрицею ваг, вказує на наявність конкретної похилої лінії в оброблюваному шарі і визначає її (лінії) координати, формуючи карту ознак. Ядра згортки формуються в процесі навчання мережі самостійно методом звичайного розповсюдження помилок. Ваги навчаються під час тренування мережі, фільтри на поточному шарі використовуються для здійснення крос-кореляції з картами ознак попереднього шару.

Отже пулінг шар розбиває зображення , що отримано від згорткового шару на невеликі ділянки , квадрат 2х2 та залишає піксель зі більшим значенням, після такого кількість пікселів зменшується у рази і нейрони наступного шару виділяють більш загальні ознаки зображення. Операція пулінгу показана на рис .3.6.



а б

а) функція pooling для обробки краю зображення

б) функція максимуму (max pooling)

Рисунок 3.6 – Операція пулінгу

Повторюючи кілька разів операції згортки і пулінгу, будується ЗНМ, складається карта ознак, що після кількох шарів стає вектором або скаляром, але їх може бути сотні, на виході мережі додають декілька шарів мережі персептрону, на вхід якої подаються кінцеві карти ознак. Отже кожен фільтр виконує згортку за всіма напрямами по ширині і висоті вхідного об'єма, розраховує скалярний добуток даних фільтра та вхідних даних, формує двовимірну карту активації для фільтрів, фільтри активуються для кожного типу ознак , частіше, у співвідношенні один до двох, якщо є карта попереднього шару (рис.3.6).

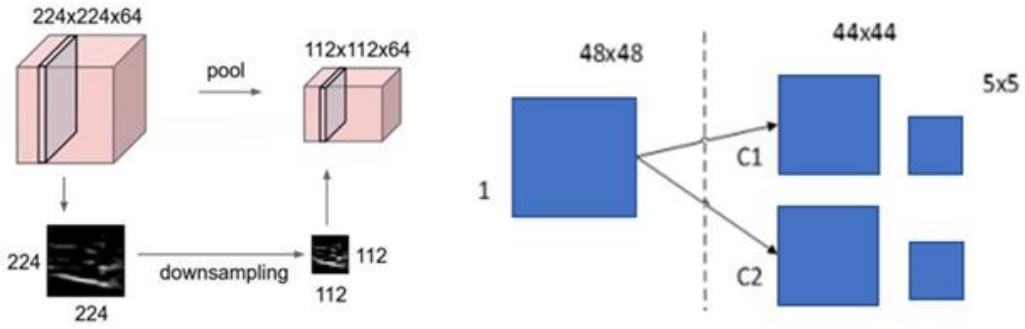


Рисунок 3.7 – Формування тривимірної або двовимірної карти активації для фільтрів зі збереженням виділених ознак

Згортка для обробки зображень описується за наступною формулою :

$$(f \times g)[m,n] = \sum f[m-k,n-l] \times g[k,l], \quad (3.1)$$

де f – вихідна матриця зображення ;

g – ядро (матриця згортки).

Згортковий шар описується такою формулою :

$$x^l = f(x^{l-1} * k^l + b^l), \quad (3.2)$$

де l – вихід шара l

$f()$ – функція активаціїї;

k^l – ядро згортки;

b^l – коефіцієнт зсуву.

Крайові ефектиv зменшують розміри вихідних матриць , таке зменшення обраховується за такою формулою:

$$x_j^l = f(\sum_i x_i^{l-1} * k_j^l + b_j^l) \quad (3.3)$$

де x^l_j – карта ознак j(вихід шара l);

$f()$ – функція активації;

b^l_j – коефіцієнт зсуву для карти ознак j ;

k^l_j – ядро згортки з номером j;

x_i^{l-1} –карти ознак з попереднього шару.

Отже однією з ключових характеристик ЗНМ є ядро, що визначає систему, у якій ваги розподілені. У згортковій мережі загальна інформація дозволяє зменшити кількість зв’язків чим забезпечується можливість виявлення типу ознаки по всій області зображення на відміну від звичайної багатошарової мережі, де велика кількість зв’язків між нейронами тягне за собою наявності синапсів, що замінює процес виявлення ознак.

За архітектурою зв'язків нейронів у нейромережі, для більшості відомих нейромереж можна згрупувати у два великі класи [17] (табл.3.1) .

Таблиця 3.1 – Класи нейромереж за архітектурою зв'язків нейронів

Типові архітектури нейромереж за зв'язком нейронів	
1 клас: Мережі прямого поширення	2 клас: Рекурентні межі
Персептрони	Мережа Хоппфілда
Мережа BackPropagation	Мережа Хемінга
Карта Кохонена	Двоскерована асоціативна пам’ять
Мережа зустрічного поширення	Мережа адаптивної резонансної теорії

Мережі прямого поширення, з односкерованими послідовними зв'язками, відносять до статичних, де входи нейронів отримують вхідні сигнали незалежні від попереднього стану нейромережі. Рекурентні мережі є динамічними, в них за рахунок зворотних зв'язків (петель) входи нейронів модифікуються в часі, що змінює стани мережі.

3.5 Машинне навчання

Машинне навчання, є розділом ШІ що займається побудовою та вивченням методів, що здатні самонавчатися та перенавчатися. Під навчанням нейромережі розуміється навчання за прецедентами, що має таке формулювання:

– по заданій скінченній множині об’єктів (прецедентів), що описуються набором даних, що збираються для кожного із прецедентів, потрібно виявляти та відновлювати певні взаємозв’язки й закономірності;

– сукупність таких прецедентів із заданим характерним описом називають навчальною вибіркою;

– під час навчання за прецедентами фіксується функціонал якості, що є критерієм якості побудованої моделі, відповідь на питання, як добре описано вхідні дані та з якого класу обрано фінальний алгорититм;

– фінальний алгоритм, що обрано у процесі навчання, приймає оптимальне значення функціоналу якості по навчальній виборці.

Виділяють декілька основних типів машинного навчання з приводу як вони використовуються для розпізнавання відбитків пальця на основі штучного інтелекту (AI).

Контрольоване навчання зазвичай використовують для розпізнавання відбитків пальців для навчальних моделей для класифікації відбитків пальців на основі позначених навчальних даних. Приклади алгоритмів:

– опорні векторні мережі (SVM),

– k-найближчі сусіди (k-NN),

– нейронні мережі.

Неконтрольоване навчання використовується ля кластеризації та пошуку шаблонів у немаркованих даних відбитків пальців. Напів контрольоване навчання використовується, коли є обмеження на кількість даних і велика кількість непозначених даних, це навчання під наглядом та без.

Алгоритми Q-Learning, Deep Q Networks (DQN), Proximal Policy Optimization використовують для навчання з підкріпленням для сценаріїв підвищення якості зображення відбитків в розпізнаванні відбитків пальців на нейромережі при взаємодіє з середовищем для зворотнього зв’язку з підвищення продуктивності з часом[17,18].

Згорткові нейронні мережі (CNN), рекуррентні нейронні мережі (RNN), мережі довготривалої короткочасної пам’яті (LSTM), сіамські мережі. та інші глибокі архітектури підходять для вилучення ознак із класифікацією відбитків пальців. Покращення продуктивності моделей розпізнавання відбувається шляхом навчання НМ, таких як Res Net, VGG .

Отже в наш час нейронні мережі стали інструментом для створення умов кращої безпеки для різних систем і галузей :

– інформаційна безпека. Нейронні мережі можуть аналізувати атаки на веб-сайти, різні програмні мобільні застосунки, спроби несанкціонованого доступу в банківських системах та інше події ;

– фізична безпека. Біометрична аутентифікація за відбитками пальців або розпізнавання обличчя, використання сканерів відбитків або аналізатори для голосової автентифікації в рази підвищили рівень безпеки доступу до систем з контролем доступу;

– аналіз аудіо звуку, НМ аналізують аудіо-сигнали і звукові сигнали в середовищі з метою виявлення небажаних подій, крики про допомогу , звуки стрільби-вибухів, будь-які незвичні звуки , що пов’язані з ситуацією «SOS»;

– візуальний моніторинг простору і відеоспостереження. НМ аналізують великі обсяги відеопотоків з метою виявлення небажаних вторгнень, або активності людей з небезпечною поведінкою, тощо ;

– аналіз та прогнозування загроз. НМ прогнозують аналізуючи великі обсяги вхідних даних для виявлення потенційних загроз і ризиків для подій в різних система [11, 18]

Із всього що сказано вище про НМ можна зробити висновок, що інтеграція і налаштовування їх так, щоб вони надавали безпомилкові результати є можливою. НМ створюють моделі, що навчаються виявляти патерни та зв’язки, постійно покращують здатність в роз’язанні великих завдань, її можна реалізувати за архітектурою RNN, CNN, або комбінацією різних архітектур.

В наш час , у 2025 році, нейромережі є потужним засобом для різних технологій разом зі штучним інтелектом мають хороший потенціал для подальшого розвитку в аналізі даних для систем розпізнавання і прогнозування і багатьох інших сферах життя таких як автоматизація процесів та безпека.

4 РОЗРОБКА МОДЕЛІ СИСТЕМИ РОЗПІЗНАВАННЯ ВІДБИТКІВ ПАЛЬЦІВ НА ОСНОВІ НЕЙРОННОЇ МЕРЕЖІ

4.1 Вибір нейронної мережі для проведення дослідження

Для побудови основної сіамської мережі у дослідженні використовувалась платформа PyTorch, вхідний рівень каналу 128×128×3. Дві основні мережі були експортовані до функції втрат.

Функція втрат, яка використовувалась у цьому дослідженні, була контрастною втратою. Такий тип функції втрат є ефективним для обробки зв'язку між виходами двох основних мереж у сіамських мережах. У такому випадку мінімальна відстань втрати становить:

$$\frac{1}{2N}\sum_{n=1}^{N} yd^2 + (1-y)(margin - d, 0)^2 \tag{4.1}$$

Виведена векторна відстань L, повністю зв'язана двічі після обчислення функції втрат, а вихідний рівень приймає сигмоподібну функцію для нормалізації отриманих значень. У цьому випадку мережа є мережею порівняння. Якщо співпадіння між двома зображеннями є високим, вихідні дані зміщуються до 1. В іншому випадку вихідні дані зміщуються до 0.

У даному дослідженні була навчена сіамська мережа за допомогою 8 різних відбитків пальців. Для цього використовували зображення відбитків пальців розміром 128×128. Зображення відбитків одного й самого пальця в навчальному наборі були згруповані та зберігалися в одній папці. Для базової мережі VGG у цьому дослідженні застосовувалися попередньо навчені ваги VGG16, які використовувалися для подальшого донавчання моделі. У навчальному наборі представлено чотири типи зображень відбитків пальців,

що відповідають різним пальцям і були отримані за допомогою пристрою збору відбитків AS60x. Для кожного окремого відбитка пальця до навчального набору було відібрано по три зображення (рис. 4.1). Усі зображення навчального набору були попередньо оброблені, кожне зображення відбитка пальця піддавалося п’яти операціям згортки, результат – сформовано три додаткові зображення (рис. 4.1), середня кількість зображень для кожного відбитка пальця зросла до шости.

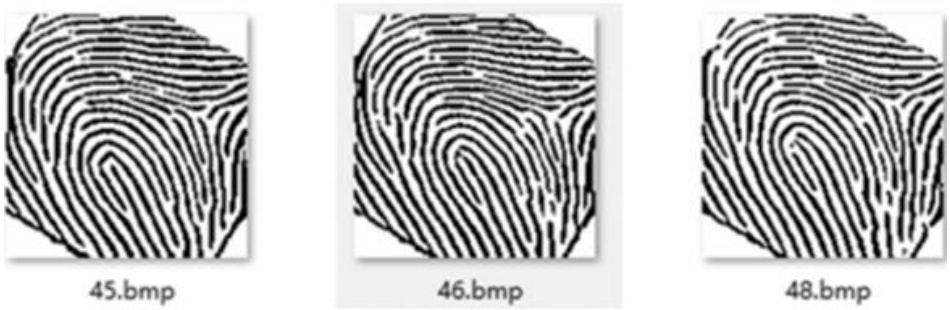


Рисунок 4.1 – Сформовані три додаткові зображення

Щодо навчання порівняльної мережі, з навчального набору відбиралися два зображення одного й того самого типу, для яких вихідне значення встановлювалося рівним 1. У разі вибору зображень різних типів вихід калібрувався до 0, аналогічно підходу, описаному в попередніх розділах. Далі послідовно відбиралися інші пари зображень різних типів, повторювався попередній крок і здійснювалося формування навчального набору. Після такого навчання, якщо на вхід мережі подавалися два зображення відбитків одного пальця, її вихідне значення наближалося до 1; у протилежному випадку, коли зображення належали різним пальцям, вихід мережі прямував до 0.

Параметри та результати процесу навчання були такими:

– розмір пакета (batch size) становив 32;

– швидкість навчання – 0,001;

– кількість епох – 1000;

– значення загальної функції втрат –0,1149;

– тривалість навчання – 3 дні;

– час тестування на один період – 600 мс.

Стандартний алгоритм Гальтона було застосовано до бази даних попередньо оброблених зображень, запропонованої в цьому дослідженні. Отримані результати підтвердили сумісність запропонованої бази даних із традиційними системами, що дало змогу успішно реалізувати цільову систему.

У роботі запропоновано метод зіставлення зображень на основі вбудованої сіамської нейронної мережі, який застосовується для порівняння відбитків пальців. Запропонований підхід дає змогу виконувати розпізнавання відбитків пальців з будь-яких джерел (баз даних, фотографій або зображень) із використанням вбудованого алгоритму обробки зображень, що дозволяє відмовитися від окремого етапу формування бази даних відбитків.

На відміну від традиційних методів розпізнавання відбитків пальців, які потребують виділення мініцій та їх подальшого зіставлення, підхід на основі сіамської нейронної мережі здійснює ідентифікацію шляхом безпосереднього порівняння зображень відбитків пальців і формування числового показника їхньої подібності.

4.2 Обумовлення вибору програмних засобів для розв’язання завдання

Для розробки та реалізації методу ідентифікації відбитків пальців на основі нейроної мережі з використанням CNN було обрано наступні програмні засоби: Python, Matlab з комплексом Residual Network 50, Android Studio Java.

Програмне забезпечення Matlab для нейромереж дозволяє створювати та моделювати, розробляти за допомогою застосунків штучних нейромереж , ШІ і технологій машинного навчання для реалізації розв’язання завдання побудови системи безпеки за відбитками пальців.

Matlab є системою автоматизації математичних обчислень, з використанням матричних операцій для розв'язання завдань з лінійної алгебри

та математичного моделювання динамічних і статичних систем та об’єктів , також має багато спеціалізованих інструментів для обробки сигналів, обробки зображень, машинного навчання, статистика, динамічне моделювання оптимізація та інші. Matlab використовує свою мову та пов'язаний з мовами C, C++, Java, Python, використання його для розробки складних програмних систем і реальних застосунків для вбудованих систем. Matlab дозволяє розгортати треновані моделі нейромереж, підтримує паралельні обчислення, що є важливим для тренування великих моделей НМ. Він має вбудовані інструменти та бібліотеки для глибокого навчання:

- Deep Learning Toolbox, функції що необхідно нам для створення, тренування та валідації глибокої нейронної мережі;

- Simulink,

- Signal Processing Toolbox та інші.

Matlab має функції відображення архітектури нейромережі, відстеження кривих навчання та візуалізації ваг моделі. Функції Deep Learning Toolbox у Matlab підтримують деякі спеціалізовані апаратні засоби, такі як FPGA та SoC, для прискорення виконання деяких операцій, надає попередньо створені бітові потоки для запуску різноманітних мереж глибокого навчання на підтримуваних пристроях AMD та Intel FPGA та SoC. Інструменти Deep Learning Toolbox надають можливості для дослідження та розробки глибоких нейронних мереж у Matlab. Він має підтримку згорткових мереж (CNN), рекурентних мереж (RNN), він також має можливості для передачі навчання та використання попередньо навчених моделей, що є важливим для тренування мережі.

Python є однією з найпопулярніших мов програмування для роботи з нейронними мережами та глибоким навчанням. Його розширена екосистема бібліотек та інструментів робить його популярним вибором для розробників та дослідників. У мові Python існує кілька ключових бібліотек для глибокого навчання: - TensorFlow, розроблений Google для створення моделей машинного навчання, що можуть працювати в будь-якому середовищі.

- PyTorch, для підтримки графічних процесорів для прискорення обчислень у нейромережах і є найбільш популярними.

- Keras, що інтегрується з TensorFlow, надає високорівневий інтерфейс для швидкої розробки нейромережі.

Імпортується TensorFlow у свою програму дуже просто:

import tensorflow as tf

print("TensorFlowversion:", tf._version_)

Для створення моделі машинного навчання використовується фрагмент коду (рис. 4.2):

```
model = tf.keras.models.Sequential([
  tf.keras.layers.Flatten(input_shape=(28, 28)),
  tf.keras.layers.Dense(128, activation='relu'),
  tf.keras.layers.Dropout(0.2),
  tf.keras.layers.Dense(10)
])
```

Рисунок 4.2 – Код для створення моделі навчання

Model.evaluate цей метод перевіряє продуктивність моделі на валідаційному або тестовому наборі даних:

model.evaluate(x test, y test, verbose=2)

Класифікатор зображень тепер навчений з точністю ~98% на цьому наборі даних. Для того, щоб наша модель повертала ймовірність, необхідно обгорнути навчену модель та приєднати до неї softmax:

probability_model = tf.keras.Sequential([

model,

tf.keras.layers.Softmax()

])

Модель поверне ймовірність :

probability_model (x_test[:5])

Отже, дуже просто навчити модель машинного навчання, використовуючи попередньо створеним набором даних за допомогою API Keras.

Для обробки зображеньвикористано мову Python, що використовує бібліотеки OpenCV та Pillow. Всі аргументи, що вище було викладено, роблять мову Python зручною для розробки та дослідження нейромереж, за її простоту та широкі можливості.

Для розв’язання завдання розглянули архітектуру глибокої ЗНМ ResNet-50, що підходить для задач комп’ютерного зору, виявлення об’єктів і сегментації, також класифікації зображень – є архітектурою глибокої згорткової нейронної мережі, що використовує "залишкові блоки" (residual blocks), які дозволяють ефективно тренувати глибокі мережі. Традиційною проблемою глибоких мереж є зниклі або вибухаючі градієнти, що робить складним навчання, тренування глибоких моделей, що вирішується залишковим навчанням за допомогою з'єднань скорочення (skipconnections) за рахунок прокладання інформаційного потоку безпосередньо від одного шару до іншого. Залишкове навчання використовує бутельні структури в своїй архітектурі зі згортками 1x1, 3x3, таке з'єднання-скорочення усуває проблему зникання градієнту. ResNet-50 використовує глобальне середнє згладжування замість традиційно повних з'єднаних шарів в кінці мережі.

4.3 Розробка алгоритму роботи системи та програмна реалізація розпізнавання відбитків пальців

Схематично роботу нашої системи розпізнавання відбитків пальців на нейромережі з багатошаровою структурою можна представити наступною схемою (рис. 4.3).

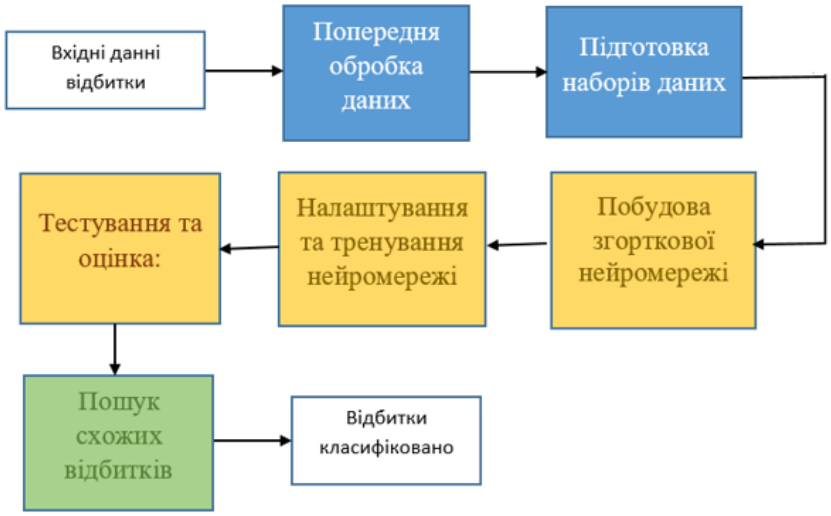


Рисунок 4.3 – Схема роботи системи розпізнавання відбитків на нейромережі з багатошаровою структурою

Опис алгоритму роботи системи, що розробляється:

– попередня обробка даних – завантажені зображення відбитків пальців піддаються попередній обробці з урахуванням покращення якості та чіткості контурів за алгоритмом Canny, що підходить для виділення ключових особливостей;

– підготовка наборів даних – дані розділяються на навчальний і тестовий набори, що дозволяє визначити ефективність тренування для оцінювання моделі, після попередньої обробки зображення зберігаються в новій директорії для зручності подальшої роботи з ними;

– побудова згорткової нейромережі – за визначеною архітектурою, що має: шар входу, згорткові шари для вилучення особливостей, ReLU-шари для активації нелінійних властивостей, та шар класифікації, що є результатом пошуку;

– налаштування та тренування нейронної мережі – визначаються параметри тренування: кількість епох, розмір пакету-batch size, функція втрат;

– тренування нейромережі на навчальному наборі для виявлення ключових особливостей і створювання шаблонів відбитків пальців;

– тестування і оцінка – тестовий набір перевіряє точність і ефективності моделі, що використовується для класифікації відбитку, показує наскільки правильно модель розпізнає відбитки пальців на нових зображеннях;

– пошук схожих відбитків пальців – навчена модель після класифікації кожного нового зображення відбитку пальця надає результат класифікації про співпадіння конкретного відбитку пальця, або його відмінність від тих зображень, що є в базі шаблонів.

Для реалізації алгоритму роботи системи розпізнавання відбитків пальців зручно використовувати комп'ютерну модель для розв'язання завданнях ідентифікації доступу, бо у подальшому є можливість для її розширення для більшої кількості масивів даних, а також для використання різних підходів навчання мереж.

Для навчання нейромережі використовуємо датасет, його створено з 4000 зображень-фото формату .png відбитків пальців (рис. 4.4), що дані приведені до однакового розміру, кольорові фото перетворено у чорно-білі для усунення різностей форматів зображень для спрощення коду розпізнавання.

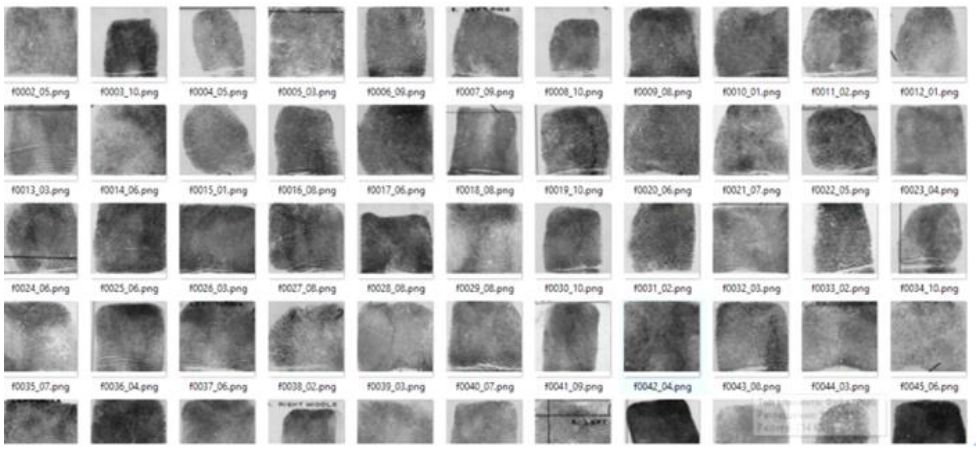


Рисунок 4.4 – Датасет відбитків у форматі .png

Також було застосовано підходи для зменшення кількості обмежувальних контурів для набору тренування НМ, що збереже час

перенавчання (overfitting) при підвищенні обсягу даних. Робоча область проекту визначається безпосередньо в Matlab на локальному ПК.

Для масштабування зображень, отримання єдиної розмірності фото 224x224 було використанно Python-скрипт (рис 4.5) .

```
inputSize = [224, 224, 3];
YPred = classify(net, imdsTest, YTest = imdsTest.Labels;
function data = readAndPreprocessImage(files, inputSize)
     data = zeros([inputSize, numel(files)], 'uint8');
          parfor i = 1:numel(files) img = imread(files{i});
          img = imresize(img, inputSize(1:2));
          data(:, :, :, i) = img;
```

Рисунок 4.5 – Функція попередньої обробки зображень відбитків

Після перетворення скриптом кольорових зображень в чорно-білі формат зображень стає 224x224x3 та зберігаються у робочій директорії окремо в папочці Resize Dataset, що стандартизує формат та розміри зображень для навчання нейромережі.

4.4 Вибір методів для виявлення контурів, алгоритм SURF

Перед передаванням даних на вхідний набір до нейронної мережі використаємо декілька методів для виявлення контурів, їх розширення за допомогою морфологічних операцій та визначення важливих точок завдяки алгоритму SURF для покращення обробки зображень.

Методи підготовки зображень із датасету описано у фрагменті коду, що показано на рисунку 4.6.

```
gray_img = rgb2gray(img);

edges = edge(gray_img, 'Canny'); figure;
     imshowpair(img, edges, 'montage'); title('Виявлені
     контури');
     se = strel('disk', 5); % edges gray;
     dilated_edges = imdilate(edges, se);
          figure;
          imshowpair(img, dilated_edges, 'montage');
          title('Розширені контури');
```

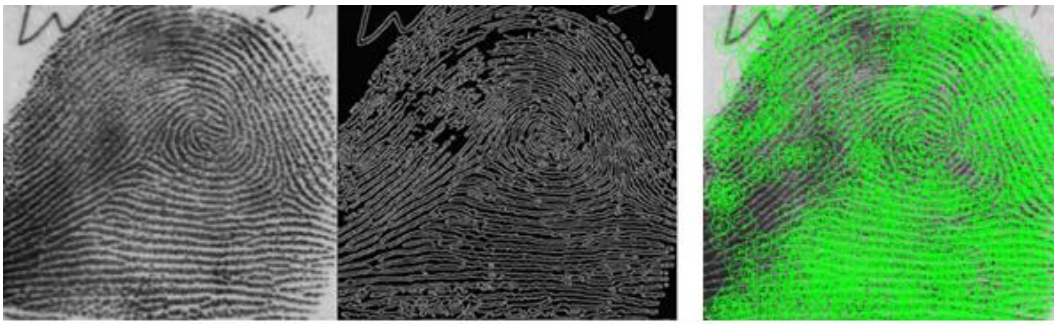
Рисунок 4.6 – Методи виявлення контурів і розширення їх

Функція SURF виконує важливу роль в області обробки відбитків пальців, використовуючи ретельну наукову методологію. Зазвичай це називають "відокремленням високорівневих ознак", вона здатна відокремлювати важливі аспекти відбитка пальця, відкидаючи нечіткі лінії, плями та шуми (рис. 4.6, б) [15]. Науковий підхід використання цієї функції полягає у використанні алгоритму Canny для виявлення контурів, що дозволяє вирізати фон та виділити ізолювати основний об'єкт інтересу [11, 23], а саме робочу область на фото, що містить відбитки пальця.

Щодо функції розширення контурів на основі морфологічних операцій– цей процес надає можливість виділяти ключові структурні елементи відбитка, (лише найсуттєвіше зображення відбитка пальця), що допомагає в підготовці даних для подальшого аналізу.

Визначення важливих точок відбувалося за допомогою алгоритму SURF. Алгоритм SURF (Speeded-Up Robust Features) є методом для визначення важливих точок на зображенні, який відноситься до області комп'ютерного зору та обробки зображень. Цей алгоритм розроблений для забезпечення ефективності та стійкості в порівнянні з іншими методами, такими як SIFT (Scale-Invariant Feature Transform). Використовується гаусівська фільтрація для створення простору масштабів для зображення.

Алгоритм аналізує зображення на різних масштабах, що дозволяє виявляти ключові точки в різних розмірах та стійкості до змін масштабу. Алгоритм відмічено високою ефективністю та швидкістю обчислень, що підходить для завдань реального часу та великих обсягів даних [15]. Роботу алгоритму виділення ознак відбитків продемонстровано візуально на рисунку 4.7.



а б в

а) зображення вирізаного фону із ізольованим об'єктом інтересу за Canny;

б) результат "відокремлення високорівневих ознак";

в) результат роботи алгоритму, виявлено ключові точки візерунка відбитка

Рисунок 4.7 – Робота алгоритму виділення ознак з зображення відбитка

4.5 Навчання нейронної мережі та результати

В код програми вносяться дані для навчання, навчена модель зберігається у проекті, результатом роботи нашої моделі є графіки втрат та точності (рис 4.7)

Втрати представляються функцією Loss, що є метрикою для визначення прогнозів і надає інформацію у вигляді графіку точності прогнозу у процентах. Завдання цієї функції знизити значення метрики втрат, або мінімізація втрат протягом ітерацій під час навчання при збільшенні кількості пройдених епох. Якщо крива Loss втрат знижується потягом навчання, це означає, що модель покращує здатність прогнозування.

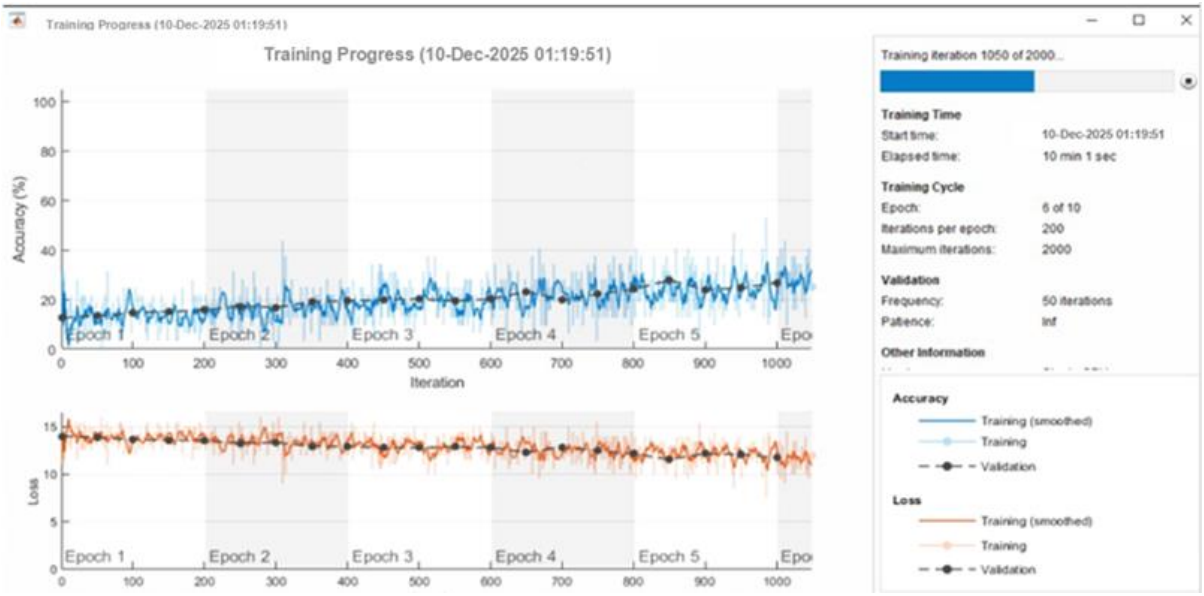


Рисунок 4.8 – Графіки навчання нейромережі

Точність моделі представлено функцією Accuracy, що є відношенням кількості правильних прогнозів да загальної їх кількості, ця функція надає інформацію у вигляді графіку точності прогнозу у процентах. Завдання цієї функції збільшити значення точності , значить крива що йде вгору позначає збільшення точності при навчанні, покращується відтворення патернів для даних, та визначення моделлю закономірностей зміни у даних у нашому випадку рисунок зображення відбитків пальців.

Є ще одна функція втрат на валідації Validation Loss , вона є величиною втрат для оцінки даних на окремому наборі. Вона використовується для об'єктивної оцінки ефективності мережі на даних, що бачить вперше. Її використовують для виявлення ознак для перенавчання моделі для більшої адаптації. Ми її не використали при навчанні нашої моделі. Але знаємо що є можливість перенавчання дописавши трошки коду. Перенавчання надає можливості перевірити, як точно наша мережа запам’ятала зображення відбитку. Але із двох отриманих графіків бачимо, що наша модель працездатна. Навіть з перших епох метрики наближаються до 100%.

В результаті розробленої системи отриманий відбиток передається із застосунку Android dateset , обробляється, вже описаним вище, алгоритмом , та багатошарова нейромережа здійснює пошук зображень, що збігаються за ознаками, із базового датасету. Знайдений код зображення використовується класифікатором net, було використано паралельний цикл parfor для пошуку схожих зображень та паралельної обробки зображень. Після обробки паралельним цикл parfor результати зконвертовано у масив, відсортований за відстанню, і перші п’ять та базове зображення відбитків виведено у якості результату розпізнавання в інтерфейсі Matlab (рис. 4.9).

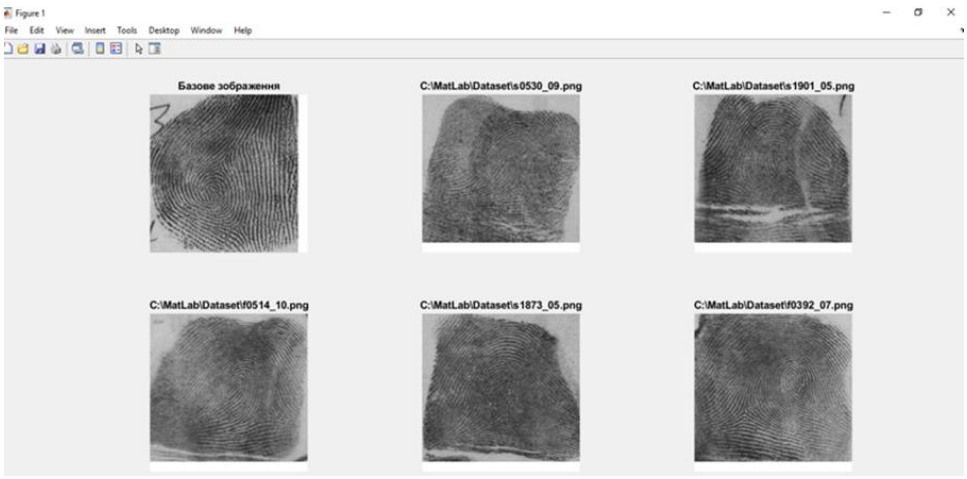


Рисунок 4.9– Результат роботи системи розпізнавання відбитків найбільше схожих на базовий

Після повторної перевірки, з 5 зображень залишається тільки два:

 – базове, надане в датасет для ідентифікації;

– друге те, що вже було у базі даних.

Таким чином – зображення відбитку ідентифіковано; доступ дозволено, або відмовлено, якщо ні одне із зображень не було знайдено.

ВИСНОВКИ

У даній кваліфікаційній роботі досліджена система розпізнавання відбитків пальців за допомогою нейронної мережі з багатошаровою структурою.

Для реалізації поставленої мети було проведено дослідження методів і технік біометричної ідентифікації людини за відбитками пальців із зображенням папілярних ліній, досліджено методи обробки цифрових зображень, архітектури нейромережі з багатошаровою структурою та розглянуто можливостей машинного навчання для розпізнавання відбитків і алгоритми обробки цифрових зображень.

Практична цінність полягає у використанні згорткових нейронних мереж для підвищення точності та стійкості в роботі системи розпізнавання на великих об’ємах даних відбитків пальців , також згорткова нейронна мережа Resnet здатна до навчання на обмеженому обсязі навчальних даних коли збір даних ускладнено.

Наукова новизна в даному досліджені полягає у використанні сіамської нейронної мережі, що є придатною, для обробки обсягів даних відбитків пальців з виявленням складних патернів незалежно від типу вхідного зображення із-за використання двох однакових мереж для паралельного навчання, що полегшує виконання завдання зменшити розрив значень характеристик між порівнюваними зображеннями.

Розглянуто найбільші проблеми, що виникають в області ідентифікації, а також розглянуто тенденції розвитку систем біометричної ідентифікації з розпізнавання відбитків пальців, що базуються на нейронних мережах з багатошаровою структурою.

Впровадження таких систем в практиці має значно підвищити рівень безпеки та зручності в системах контролю доступу до корпоративних систем,

фізичних об'єктів, мобільних пристроїв та інших сфер, де необхідний надійний контроль та безпека несанкціонованого доступу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Технологія Face ID від Apple, Як це працює https://www.google.com/search?

2. Deep MasterPrints - алгоритм, який вміє створювати зображення універсальних відбитків пальців https://ukr.media/science/379039/

3. Пристрої біометричної ідентифікації SpeedFace https://zkstore.com.ua/p2127006060-sistema-kontrolya-dostupa.html?source=merchant_center&gad_source

4. Безпечність технології Face ID https://pingvin.pro/gadgets/article-gadget/face-id-naskilky-bezpechno.html

5. Системи доступу на нейромережах https://overlook.expert/biometricheskaia-sistema-kontrolia-dostupa-inbio-odnostoronniaia-dver/

6. Сканери відбитків пальців

https://ktc.ua/blog/yak_pracyuyut_skaneri_vidbitkiv_palciv_yemnisni _optichni_ ta _ ultrazvukovi.html

7. Парціале, Д.; Чен, Ю. Передові технології безконтактного розпізнавання відбитків пальців. In Handbook of Remote Biometrics ; Springer: Лондон, Великобританія, 2009; С. 83–109.

https://link.springer.com/chapter/10.1007/978-1-84882-385-3_4

8. Рагхавендра, Р.; Буш, К.; Ян, Б. Масштабована надійна перевірка відбитків пальців за допомогою камери смартфона в реальних сценаріях. У матеріалах шостої міжнародної конференції IEEE 2013 з біометрії: теорія, застосування та системи (BTAS), Арлінгтон, штат Вірджинія, США, 29 вересня–2 жовтня 2013 р.

Режим доступу: https://ieeexplore.ieee.org/abstract/document/6712736

9. Застосування сіамських нейронних мереж для порівняння аерофотознімків із картами місцевості. (2024). / Власенко В.О. // Вісник

Національного технічного університету "ХПІ", 2024, №1-2(11-12), ISSN2079-0031 (Print) ISSN2411-0558 (Online) DOI: https://doi.org/10.20998/2411-0558.2024.01.12

http://pim.khpi.edu.ua/article/view/308457/299971

10. Методи ідентифікації людини

https://library.nlu.edu.ua/POLN_TEXT/KNIGI/1_DISKI/KRIM/html/

11. Штучні нейронні мережі. Зв'язки нейронів в нейромережі https://learn.ztu.edu.ua/pluginfile.php/176771/mod_resource/content/1.pdf

12. Персептрон https://www.simplilearn.com/tutorials/deep-learning-tutorial/perceptron#perceptron

13. Багатошаровий персептрон https://thetransmitted.com/adlucem/shho-take-mlp-u-mashynnomu-navchanni/

14. Рекурентні нейронні мережі LSTM

https://www.vpnunlimited.com/ua/help/cybersecurity/gru?srsltid

15. Алгоритм SURF та SIFT

https://pzs.dstu.dp.ua/ComputerGraphics/d&d/bibl/bioi_2015_2_14.pdf

16. Рекурентні нейронні мережі LSTM

https://www.vpnunlimited.com/ua/help/cybersecurity/gru?srsltid

17. Порівняння з LSTMs та RNNs

https://www.vpnunlimited.com/ua/help/cybersecurity/gru?srsltid

18. Архітектура зв'язків нейронів в нейромережі

https://studfile.net/preview/5740125/

19. Системи доступу на нейромережах https://overlook.expert/biometricheskaia-sistema-kontrolia-dostupa-inbio-odnostoronniaia-dver/

20. Object recognition from local scale-invariant featuresObject recognition from local scale-invariant features (1999). / Lowe D.G. // Proceedings of the International Conference on Computer Vision.

https://ieeexplore.ieee.org/abstract/document/790410

21. Olah, C. Understanding LSTM Networks. Christopher Olah's Blog. https://colah.github.io/posts/2015-08-Understanding-LSTMs/. Опубліковано: 27.08.2015

22. Каймінг Хе, Сянгю Чжан, Шаочінг Жен і Джіан Сун. Глибоке залишкове навчання для розпізнавання зображень(2016). Конференція IEEE/CVF з комп'ютерного зору та розпізнавання образів 2016 року)

https://cvpr.thecvf.com/

23. О. Фразе-Фразенко, А. Вакула Аналіз класичного алгоритму Canny щодо виділення контурів об‘єктів ідентифікації у системах захисту інформації

https://dspace.oneu.edu.ua/server/api/core/bitstreams/4f81ffa8-36f9-474f-9193-1a26f16580cf/content