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)_____
(рівень вищої освіти)

_____Методи розпізнавання відбитків пальця за допомогою_____
_____нейронної мережі для системи доступу до фізичних об'єктів_____
(тема)

Виконав: студент 2 курсу, групи СКСм-22-1
_____Корсун Д.М._____
(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 доцент Рожнова Т.Г.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ___Чумаченко С.В.__
(підпис) (прізвище, ініціали)

2023 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

(шифр і назва)

Тип програми Освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Освітня програма Спеціалізовані комп'ютерні системи

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. Кафедри АПОТ _____

(підпис)

«____»_____ 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Корсуну Денису Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Методи розпізнавання відбитків пальця за допомогою нейронної мережі для системи доступу до фізичних об'єктів

затверджена наказом по університету від 03 листопада 2023 р. № 1282 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 19 січня 2024 р.

3. Вихідні дані до роботи

Методи ідентифікації особистості

Архітектура нейронної мережі

Методи для аналізу та обробки зображень

Великі масиви даних

Алгоритми роботи штучних нейронних мереж

4. Перелік питань, що потрібно опрацювати в роботі

Мета роботи

Аналіз нейронних мереж для розпізнавання відбитків

Архітектура нейронних мереж

Огляд методів розпізнавання відбитків пальців

Вибір програмних рішень та технологій

Аналіз ефективності можливих рішень застосування розпізнавання відбитку

Результати досліджень

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____
слайди презентацій – 11 слайдів .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

7. Дата видачі завдання _____20 жовтня 2023р._____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Вибір теми роботи, затвердження теми	20.10.2023-25.10.2023	
2	Аналіз предметної області	26.10.2023-30.10.2023	
3	Аналіз існуючих рішень	31.10.2023-05.11.2023	
4	Вибір методів для ідентифікації відбитків пальця	06.11.2023-15.11.2023	
5	Аналіз використання нейронних мереж в зазначеній області	16.11.2023-23.11.2023	
6	Приклад реалізації згорткової нейронної мережі	24.11.2023-05.12.2023	
7	Оформлення пояснювальної записки	06.12.2023-30.12.2023	
8	Оформлення графічного матеріалу	02.01.2024-05.01.2024	
9	Перевірка виконаного проекту керівником	06.01.2024-12.01.2024	

Студент _____ Корсун Д.М.
(підпис)

Керівник роботи _____ доцент Рожнова Т.Г.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 66 сторінок, 25 рисунків та 21 джерело за переліком посилань.

БІОМЕТРІЯ, ІДЕНТИФІКАЦІЯ, ЗГОРТКОВА НЕЙРОННА МЕРЕЖА, ПЕРСЕПТРОН, ФІЛЬТР ГАБОРА, ГЛИБОКЕ НАВЧАННЯ, СЕГМЕНТАЦІЯ ВІДБИТКІВ ПАЛЬЦІВ, РОЗПІЗНАВАННЯ ОБРАЗІВ.

Метою роботи є дослідження існуючих методів ідентифікації відбитків пальця за допомогою нейронної мережі з обробкою великих об'ємів даних при роботі з особливими властивостями папілярних ліній. Розробка математичної моделі для аналізу ефективної роботи обраної нейронної мережі та реалізація методу аутентифікації на основі штучних нейронних мереж в системах доступу до фізичних об’єктів.

Предметом дослідження є існуючи методи машинного розпізнавання відбитків пальців за допомогою нейронних мереж.

Об’єкт дослідження – процеси ідентифікації в системах доступу.

Проаналізовано методи та техніки розпізнавання відбитків пальця, які допомагають досягти високої точності та надійності біометричної аутентифікації. Досліджно методи попередньої обробки даних, що покращують якість навчання моделі для вдосконалення системи ідентифікації відбитків пальця на основі нейронних мереж.

ABSTRACT

The explanatory note to the certification work contains: 66 pages, 25 drawings and 21 sources according to the list of references.

BIOMETRY, IDENTIFICATION, CONVOLUTIONAL NEURAL NETWORK, PERCEPTRON, GABOR FILTER, DEEP LEARNING, FINGERPRINT SEGMENTATION, PATTERN RECOGNITION.

The purpose of the work is to analyze the existing methods of identification of fingerprints using neural networks with the processing of large volumes of data when working with the special properties of papillary lines. The development of a mathematical model for the analysis of the effective operation of selected neural networks and the implementation of an authentication method based on artificial neural networks in access systems to physical objects.

The subject of the research is the existing methods of machine recognition of fingerprints using neural networks.

The object of research is identification processes in access systems.

The methods and techniques of fingerprint recognition that help to achieve high accuracy and reliability of biometric authentication are analyzed. An analysis of the advantages and disadvantages of existing methods was carried out. Data preprocessing methods that can improve the quality of model training are considered. The direction of research is determined - improvement of the fingerprint identification system based on neural networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

MFA – багатофакторна автентифікація;

UDUFR – ультразвукове розпізнавання відбитків пальців дисплеєм;

SAW – поверхневі акустичні хвилі;

AI – штучний інтелект;

AES – розширений стандарт шифрування;

RSA – криптографічний алгоритм з відкритим ключем;

MEMS – мікроелектромеханічні системи;

SVM – опорно-векторні мережі;

PCA – аналіз головних компонент;

CNN – згорткова нейронна мережа;

DQN – глибока Q-нейронна мережа;

LSTM – мережа довгої короткострокової пам’яті;

DP – глибоке навчання;

JS – java script;

NMS – non max suppression;

ОЯЗ – оцінювання якості зображень;

RNN – рекурентні нейронні мережі.

ВСТУП

У системі безпеки та контролю доступу, що швидко розвивається, біометрична аутентифікація займає перше місце, пропонуючи високу точність і зручність. Серед різних біометричних моделей розпізнавання – ідентифікація по відбиткам пальців привернуло значну увагу завдяки своїм унікальним і відмінним характеристикам, що робить його надійним кандидатом для контролю доступу до різноманітних об’єктів в багатьох сферах. Кожен відбиток пальця представляє собою унікальний графічний візерунок доріжок та борозен, які виявляються на пальцевій подушці. Ці унікальні особливості (папілярні лінії) формуються ще в ембріональному періоді та залишаються практично незмінними протягом усього життя. Відбитки пальців використовуються для біометричної аутентифікації та ідентифікації особи в різних галузях, зокрема в безпеці, медицині, аеропортах, урядових установах та банківській сфері. Системи, які базуються на відбитках пальців, відмінно справляються з завданнями контролю доступу до приміщень, а також визначення особи для забезпечення безпеки та автоматизації процесів.

Одним з видатних вчених, який займався ідентифікацією за відбитками пальців, є Пол Ламберт. Він відомий своїми дослідженнями у галузі біометричних технологій, зокрема відбитків пальців. Його роботи стосуються алгоритмів обробки та порівняння відбитків пальців для розпізнавання особи.

Розвиток технологій, особливо у сфері штучного інтелекту, зробив революцію в методології розпізнавання відбитків пальців. Нейронні мережі, видатний інструмент у цій сфері, продемонстрували винятковий потенціал у підвищенні точності та ефективності систем ідентифікації відбитків пальців.

Ця робота присвячена дослідженню використання нейронних мереж для розпізнавання відбитків пальців у системах контролю доступу до фізичних об’єктів.

Основна мета роботи полягає в дослідженні різних архітектур і методологій нейронних мереж для оптимізації точності, швидкості та надійності ідентифікації відбитків пальців. Крім того, дослідження спрямоване на оцінку потенційної інтеграції цих передових біометричних систем у реальні програми, що забезпечить плавний та безпечний доступ до віртуальних або фізичних об’єктів.

Актуальність дослідження виявляється у забезпеченні безпеки та ефективної аутентифікації особи, яка стає критично важливою в умовах зростаючої кількості цифрових загроз та кібератак. Використання нейронних мереж для ідентифікації особи за відбитками пальців гарантує високий рівень безпеки, оскільки кожен відбиток містить унікальний рисунок та відбитки пальців майже не піддаються підробці. Також з розвитком нейронних мереж та обчислювальних технологій значно покращується швидкість та ефективність процесу ідентифікації. Це важливо для сучасних систем, які вимагають миттєвого реагування та високої продуктивності. Важливим фактором також є зростання популярності пристроїв з біометричними можливостями, які потребують ефективної інтеграції та масштабування технологій ідентифікації за відбитками пальців.

Нейронні мережі можуть бути оптимізовані для роботи на різних пристроях та у різних сценаріях використання. Подальше дослідження та вдосконалення методів ідентифікації особи за відбитками пальців за допомогою нейронних мереж може призвести до винайдення нових підходів, які поліпшують точність та надійність систем біометричної аутентифікації.

1 АНАЛІЗ АКТУАЛЬНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ ОТРИМАННЯ ДАНИХ ЗА ДОПОМОГОЮ БІОМЕТРІЇ

Біометрія виділяється як найкращий метод ідентифікації порівняно з традиційними підходами завдяки своїм притаманним властивостям. Перш за все, біометрія використовує унікальні фізичні чи поведінкові риси, властиві кожній людині, що робить їх надзвичайно відмінними та практично неможливими для точного повторення. Ці ознаки, як-от відбитки пальців, візерунки сітківки ока чи риси обличчя, не схожі на паролі чи PIN-коди, які можна забути, поділитися чи вкрасти.

Крім того, точність і надійність біометричних систем відрізняє їх від інших. Точність зіставлення біометричних даних значно зменшує межу похибки, що забезпечує більш надійний процес ідентифікації. Ця точність зводить до мінімуму помилкові спрацьовування та негативні результати, підвищуючи загальну безпеку.

Іншим переконливим фактором є те, що біометричні дані не підлягають передачі. На відміну від паролів або фізичних токенів, які можуть бути передані або використані кимось іншим, біометричні дані особи є невід’ємною частиною її істоти, що забезпечує автентичність процесу ідентифікації.

З точки зору взаємодії з користувачем, біометрія пропонує неперевершену зручність і швидкість. Простий акт сканування відбитка пальця, сітківки ока або обличчя забезпечує безпроблемний і швидкий процес автентифікації, що робить його зручним і ефективним.

Інтегрована в підхід багатофакторної автентифікації (MFA), біометрія ще більше підвищує безпеку. MFA, що поєднує біометричні дані з іншими факторами автентифікації, створює комплексну систему безпеки, яку важко зламати.

1.1 Сучасні технології розпізнавання відбитків пальця

Розпізнавання відбитків пальців, також відоме як біометрія відбитків пальців, є широко використовуваною та зрілою технологією для ідентифікації та перевірки осіб на основі їхніх унікальних шаблонів відбитків пальців. Існує багато технологій розпізнавання відбитків пальців, кожна з яких має свій підхід і методи. Опишемо деякі з ключових технологій [1].

Оптичне розпізнавання відбитків пальців використовує світло та оптику для отримання зображень відбитків пальців із високою роздільною здатністю. Зазвичай використовується в смартфонах, ноутбуках та інших споживчих пристроях. Принцип оптичного методу зображено на рисунку 1.1.

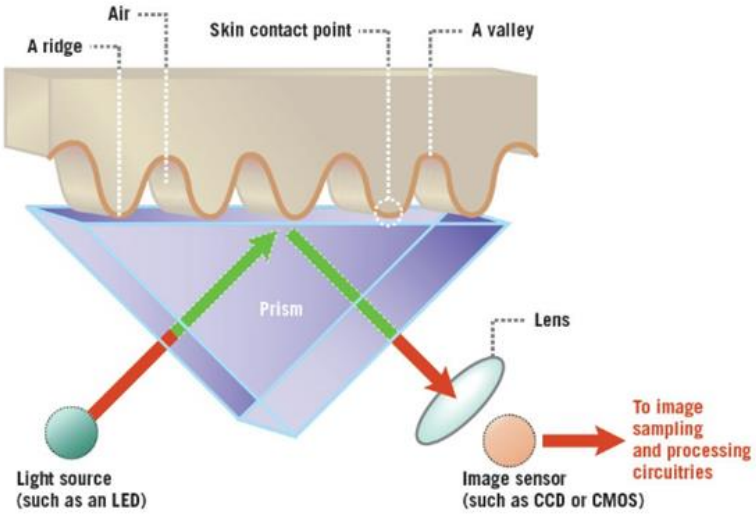

Рисунок 1.1 – Приклад розпізнавання відбитків оптичним методом

Ємнісне розпізнавання відбитків пальців для створення зображення відбитка пальця ґрунтується на принципах ємності. Зазвичай використовується в сучасних смартфонах.

Ультразвукове розпізнавання відбитків пальців Використовує ультразвукові хвилі для відображення тривимірних функцій відбитка пальця (рис. 1.2). Забезпечує більш безпечне та точне зчитування порівняно з оптичними методами.

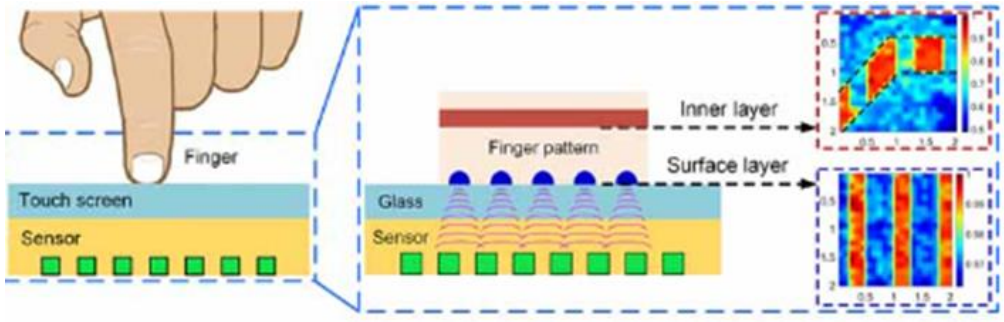

Рисунок 1.2 – Принцип роботи ультразвукового датчику на основі технології UDUFR

Теплове розпізнавання відбитків пальців використовує термодатчики для визначення унікальних теплових характеристик відбитка пальця. Може використовуватися в різних програмах для аутентифікації.

Розпізнавання відбитків пальців за допомогою натискання вимірює тиск, який чинять виступи та западини на поверхню, забезпечуючи тривимірне представлення відбитків пальців.

Розпізнавання відбитків пальців за допомогою поверхневих акустичних хвиль (SAW) Використовує поверхневі акустичні хвилі для отримання зображень відбитків пальців і створення унікального шаблону відбитків пальців (рис.1.3).

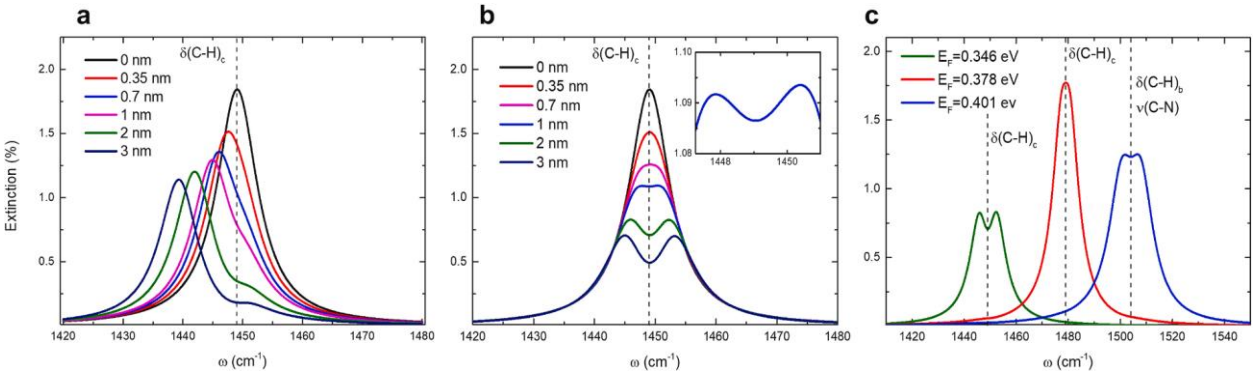

Рисунок 1.3 – Принцип роботи датчика DLG/h для зняття відбитків пальців вібраційних резонансів.

Твердотільний сканер розпізнавання відбитків пальців інтегрує датчики відбитків пальців безпосередньо в тверду поверхню (наприклад, кнопку,

дисплей) для безперебійної та непомітної аутентифікації за відбитками пальців [2].

Багатоспектральне розпізнавання відбитків пальців поєднує дані з кількох спектрів (наприклад, видимого, ближнього інфрачервоного) для підвищення якості та точності зображення відбитків пальців (рис. 1.4).

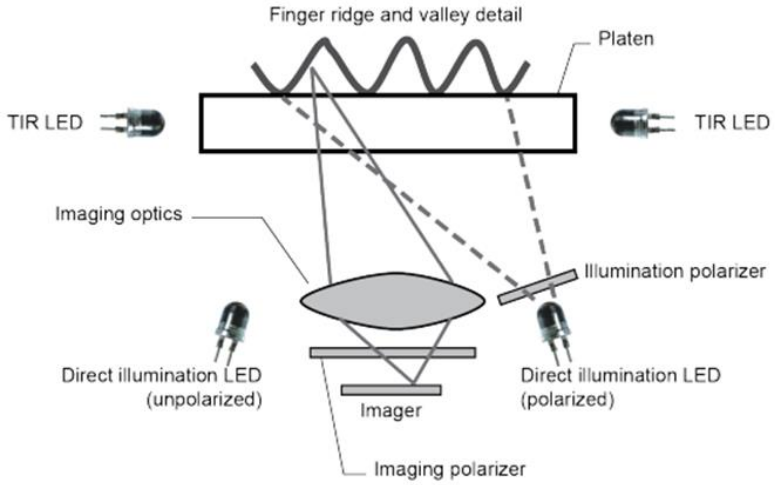

Рисунок 1.4 – Оптична конфігурація датчика MSI для багатоспектрального розпізнавання відбитку пальця

Машинне навчання та розпізнавання відбитків пальців на основі ШІ використовує алгоритми машинного навчання та штучний інтелект для покращення відповідності відбитків пальців і точності автентифікації.

Розпізнавання пальців у реальному часі включає технології для розрізнення живих пальців від підроблених відбитків пальців (виявлення підробки) для підвищення безпеки. Процес включає захоплення відбитків пальців за допомогою спеціальних сенсорів чи камер з видаленням шуму.

Технології розпізнавання відбитків пальців використовуються в різних додатках, включаючи мобільні пристрої, системи контролю доступу, банківську справу, правоохоронні органи, прикордонний контроль, охорону здоров’я тощо. Вони пропонують зручний і безпечний спосіб автентифікації людей на основі їхніх унікальних відбитків пальців.

1.2 Аналіз методів шифрування

Шифрування є важливим аспектом захисту інформації під час передачі та зберігання та відтворення. Він передбачає перетворення даних у нечитабельний формат за допомогою криптографічних алгоритмів, що робить їх недоступними для неавторизованих користувачів. Нижче описані кілька поширених методів шифрування для захисту, передачі та зберігання інформації та даних.

Симетричне шифрування використовує один секретний ключ як для шифрування, так і для дешифрування (рис. 1.5). Той самий ключ використовується для кодування та декодування даних. Приклади симетричних алгоритмів шифрування включають Advanced Encryption Standard (AES) і Data Encryption Standard (DES). Симетричне шифрування є швидким і ефективним, але воно вимагає безпечного обміну секретним ключем між сторонами, що спілкуються. Розширений стандарт шифрування (AES) – поширений алгоритм симетричного шифрування, який забезпечує надійний захист і ефективну продуктивність. AES підтримує розміри ключів 128, 192 і 256 біт. Також до методів симетричного шифрування можна віднести такі алгоритми, як Blowfish і Twofish. Це симетричні алгоритми шифрування, відомі своєю гнучкістю та високим рівнем безпеки. Вони підтримують ряд розмірів ключів, що робить їх придатними для різних застосувань [3].

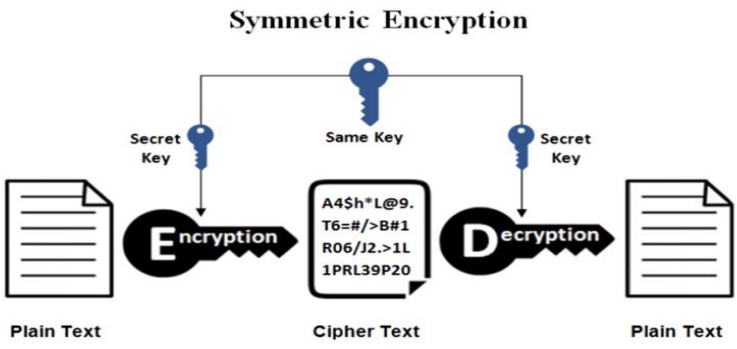

Рисунок 1.5 – Алгоритм роботи симетричного шифрування

Асиметричне шифрування (також відоме як шифрування з відкритим ключем) передбачає використання пари математично пов’язаних ключів: відкритого ключа для шифрування та закритого ключа для дешифрування. Відкритий ключ можна вільно поширювати, а закритий ключ зберігається в секреті. Дані, зашифровані за допомогою відкритого ключа, можна розшифрувати лише за допомогою відповідного закритого ключа. Популярні асиметричні алгоритми шифрування включають RSA та еліптичну криптографію (ECC). Асиметричне шифрування повільніше, але забезпечує розповсюдження ключів і переваги неспростування. ECC забезпечує надійну безпеку з меншою довжиною ключа порівняно з іншими алгоритмами, що робить його ефективним у середовищах з обмеженими ресурсами [4].

Хеш-функції – це односторонні математичні алгоритми (рис. 1.6), які генерують вихідні дані фіксованого розміру (хеш) із вхідних даних будь-якого розміру. Хеш-функція перетворює вхідні дані в унікальне, необоротне хеш-значення. Хеш-функції зазвичай використовуються для перевірки цілісності даних, зберігання паролів і цифрових підписів. Приклади хеш-функцій включають SHA-256 (алгоритм безпечного хешування) і MD5 (алгоритм дайджесту повідомлень). сімейство хеш-функцій, розроблене Агентством національної безпеки (NSA) у Сполучених Штатах. SHA-1, SHA-256, SHA-384 і SHA-512 є широко використовуваними хеш-функціями.

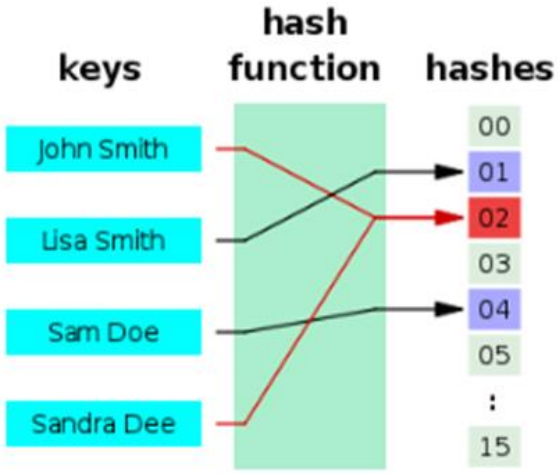

Рисунок 1.6 – Принцип роботи hash-функцій

Безпека транспортного рівня (TLS) і рівень захищених сокетів (SSL): TLS і його попередник SSL – це протоколи, які забезпечують безпечний зв’язок через Інтернет. Вони використовують комбінацію симетричного та асиметричного шифрування для встановлення безпечного з’єднання між клієнтом і сервером. TLS/SSL забезпечують конфіденційність, цілісність і автентифікацію даних. Вони зазвичай використовуються для захисту веб-трафіку (HTTPS), електронної пошти (SMTPS, IMAPS) та інших мережевих протоколів [5].

Протоколи для шифрування файлів і дисків шифрують дані в стані спокою, захищаючи їх на пристроях. Вони забезпечують шифрування окремих файлів або цілих дисків, роблячи дані нечитабельними в разі несанкціонованого доступу. Приклади включають BitLocker (Windows), FileVault (Mac) і VeraCrypt (кроссплатформенний). Diffie-Hellman (DH) – алгоритм обміну ключами (рис. 1.7), який дозволяє двом сторонам установити спільний секретний ключ через незахищений канал зв’язку. DH широко використовується в захищених протоколах зв'язку. Еліптична крива Діффі-Хеллмана (ECDH) – варіант алгоритму на основі криптографії еліптичної кривої. ECDH забезпечує подібну функціональність, але з меншою довжиною ключа, що призводить до підвищення ефективності.

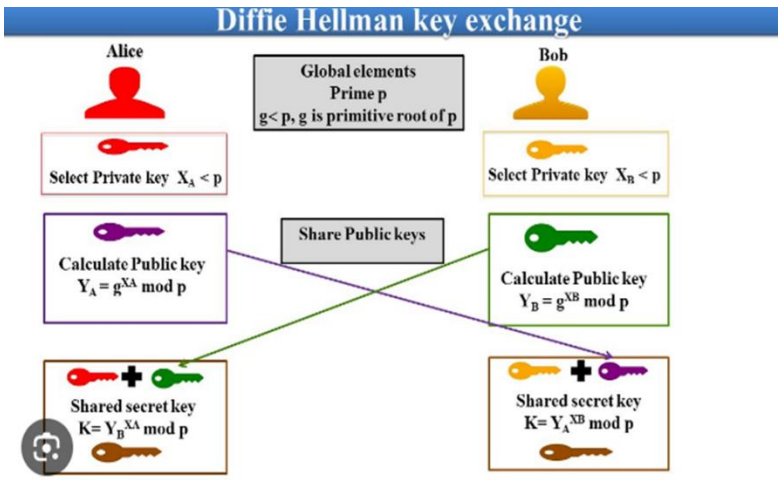

Рисунок 1.7 – Алгоритм роботи Diffie-Hellman

Гомоморфне шифрування дозволяє виконувати обчислення безпосередньо із зашифрованими даними без необхідності дешифрування. Це дозволяє обробляти конфіденційну інформацію, зберігаючи конфіденційність. Гомоморфне шифрування – це нова галузь із різними методами, такими як частково гомоморфне шифрування та повністю гомоморфне шифрування.

Це основні з існуючих методів шифрування. Вони відіграють важливу роль у захисті конфіденційної інформації під час передачі та зберігання. Вибір криптографічних алгоритмів залежить від таких факторів, як вимоги безпеки, сумісность, продуктивность та стандартів у певній галузі.

1.3 Методи порівняння відбитків пальців

Існуючі класи алгоритмів порівняння відбитків пальців можна умовно розділити на три типи: кореляційне порівняння, порівняння з папілярним візерунком та порівняння з використанням особливих точок папілярних ліній.

Метод кореляційного порівняння використовує по-піксельне порівняння двох відбитків пальців, де для одного з них відома його приналежність конкретній людині. Незважаючи на його простоту, при використанні такого алгоритму враховуються спотворення зображення та шуми, які є характерними для всіх алгоритмів порівняння відбитків пальців. У зв'язку з тим, що при знятті відбитка пальця кожного разу його положення і кут можуть відрізнятися, кореляційний алгоритм використовує складні алгоритми екстракції, обчислення ступеня схожості та порівняння з наперед заданим граничним значенням [6].

Перевагою цього методу є його простота реалізації та надійність, а також низькі вимоги до якості вихідного зображення відбитка пальця. Проте його недолік полягає в тому, що процес порівняння папілярного візерунка відбувається довго, що робить його неефективним, якщо важливим критерієм є час виконання алгоритму.

Ще один клас алгоритмів базується на аналізі будови папілярного візерунка. Зображення відбитка сегментується, а візерунок в кожному сегменті описується фрактальною функцією або синусоїдальною хвилею. Для ідентифікації в базу даних заносяться значення зсуву фази, довжини хвилі та напряму її поширення. Головні переваги цього класу алгоритмів – висока швидкість роботи та низькі вимоги до якості вихідного зображення. Недоліками цього підходу є складність реалізації та вузько-математична спрямованість, що вимагає високої математичної підготовки для реалізації. Також цей клас алгоритмів рідко використовується у системах безпеки інформаційних систем через зазначені недоліки.

Останній клас алгоритмів базується на аналізі унікальних особливостей відбитка пальця, а саме на перетинах і закінченнях папілярних візерунків. Аналіз особливих точок включає створення карти особливих точок та її порівняння з шаблоном в базі даних. Перевагами цього методу є висока швидкість і відносна простота реалізації, але недоліком є високі вимоги до якості вихідного зображення. Цей клас алгоритмів широко використовується завдяки своїй простоті та швидкості.

1.4 Алгоритм порівняння візерунка пальця за особливими точками

Для розгляду як найбільш ефективного алгоритму розпізнавання папілярних ліній за методом особливих точок можна отримати алгоритм, що ґрунтується на генерації цифрової біометричної послідовності. Цей метод відзначається високою ефективністю у завданні перетворення вхідного набору даних у бітову послідовність. Один із наукових підходів до порівняння візерунка пальця за особливими точками може бути оснований на використанні методу динамічного програмування та визначенні відстані між двома відбитками пальців. Професор Аніль К. Джайн інформаційних технології та науки про комп'ютери в Університеті штату Мічиган працював у

газулі біометрії та використовував цей метод у своїх роботах. Загальний алгоритм такого порівняння:

– витягування особливих точок. Здійснюється процес витягування особливих точок з відбитків пальців. Це може включати в себе виявлення кінців та відгалужень на папілярних лініях;

– створення візерунок пальця на основі отриманих особливих точок. Це може включати в себе використання координат, орієнтаційних даних та інших характеристик;

– формування матриці відстаней. Для кожної пари особливих точок обчислюється відстань між ними. Це може бути виконано за допомогою евклідової відстані або інших метрик відстаней;

– визначається глобальна відстань між візерунками пальців на основі отриманої матриці сумарних відстаней;

– на підставі порівнянь приймається рішення щодо ідентичності чи подібності візерунків пальців.

Цей підхід базується на принципах обробки зображень, математичних методах та криптографії. Для захисту конфіденційності та цілісності біометричних даних можуть використовуватися криптографічні методи, такі як схема "Fuzzy Vault" або інші техніки [7].

1.5 Принцип роботи та отримання інформацію за допомогою ультразвукового датчика 3d fingerprint sensor-on-a-chip

Відносно новою технологією сканування відбитків пальців, яка увійшла в простір розвитку захисту смартфонів, є ультразвуковий датчик. Компанія Qualcomm в 2022 році презентувала друге покоління нового ультразвукового 3D сканера Sonic Max [8].

Для розпізнавання відбитка ультразвуковий сканер використовує ультразвуковий передавач та приймач. Ультразвуковий імпульс передається безпосередньо на палець, розміщений перед сканером. Частина цього імпульсу

поглинається, а частина повертається до приймача і далі розпізнається залежно від гребенів, западин та інших деталей відбитка, які є унікальними кожному за пальця. В ультразвукових сканерах датчик, який виявляє механічну напругу, використовується для розрахунку інтенсивності повертається ультразвукового імпульсу в різних точках на сканері. Сканування протягом більш тривалого часу дозволяє розпізнати додаткові дані по глибині відбитка, які будуть захоплені, і дадуть дуже докладні 3D зображення відсканованого відбитка пальця. Використання 3D технології в цьому методі сканування робить його найбезпечнішою альтернативою ємнісним сканерам.

На прикладі 3D Ultrasonic Fingerprint Sensor-on-a-Chip можна розглянути детальний принцип роботи сканування.

На рисунку 1.8 показана схема пристрою, що містить пластину MEMS з перетворювачами AlN і стандартними схемами HV CMOS 0,18 мкм, приєднаними до пластини. Кожна матриця складається з масиву 110×56 прямокутних п’єзоелектриків.

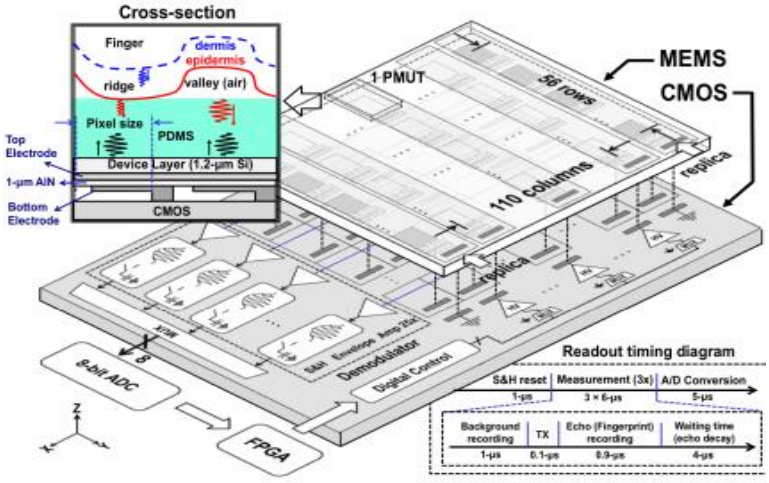

Рисунок 1.8 – Схема пристрою, що містить пластину MEMS з перетворювачами AlN

Згенероване 3-D зображення базується на акустичному відрізку часу, тому може записувати інформацію, щодо того як відбитки пальців епідермісу

та дерми на поверхні пальця створюють сильну акустичну луну на поверхні датчика через невідповідність імпедансу між повітрям (430Rayl) і PDMS (1,5MRayl). Таким чином хвиля проникає в палець і частково відбивається на шарі дерми під шкірою. Зчитування є послідовним у стовпцях і починається з фази скидання. Створення зображень починається із запису фонового зображення. Згодом усі 56 перетворювачі у вибраному стовпці збуджуються трьома імпульсами 24 В на частоті 14 МГц, створення ультразвукового імпульсу. Останні 5 мкс зчитування стовпця виділяються на аналого-цифрове перетворення. Зчитування займає 24 мкс на стовпець і 2,64 мс для всього масиву.

На рисунку 1.9 показано зображення відбитків пальців, записані в чистих умовах і з використанням поту та масла. Забруднення призводить лише до незначного погіршення зображення. Також на рисунку показані оптичні зображення датчика після того, як палець був оброблений та видалений. Хоча відбиток пальця добре видно, зчитувач однозначно відрізняє його від справжнього пальця та відповідних «підробок». Ця функція гарантує надійність проти атак спуфінгу та забезпечує високий рівень безпеки.

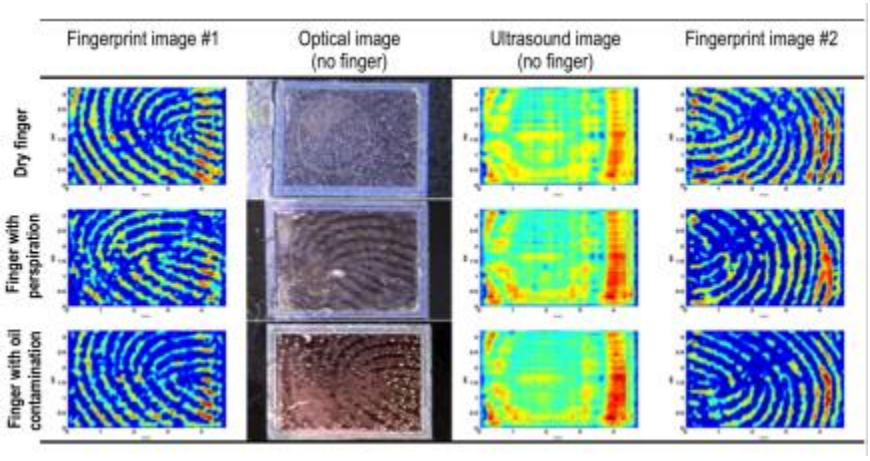

Рисунок 1.9 – Зображення відбитків пальців, записані в чистих умовах і з використанням поту та масла

Потрібно зазначити, що навіть такі, прогресивні методи ідентифікації користувача, які використовуються в сучасних смартфонах та різних

пристроях поступаються технологічності та можливостям розпізнавання біометрії за допомогою машинного навчання та штучного інтелекту.

В цьому випадку найбільш актуальними питаннями є:

– підвищення точності, так як моделі машинного навчання, особливо моделі глибокого навчання, можуть вивчати складні шаблони та особливості в потрібних відбитків пальців, які нелегко розрізнити за допомогою традиційних методів на основі датчиків. Це забезпечує більшу точність розпізнавання відбитків пальців;

– моделі машинного навчання можуть адаптуватися та розвиватися з часом. Вони можуть безперервно покращувати свою продуктивність, оскільки вони піддаються більшій кількості даних;

– розпізнавання відбитків пальців за допомогою машинного навчання може обробляти варіації зображень відбитків пальців, спричинені такими факторами, як вологість, бруд і різні умови сканування. Ці моделі часто розроблені таким чином, щоб бути стійкими до шуму та коливань;

– розширені моделі машинного навчання можуть забезпечити високий рівень безпеки, фіксуючи детальні характеристики відбитків пальців. Їх важко підробити за допомогою підроблених відбитків пальців, що викликає занепокоєння в чутливих до безпеки програмах;

– моделі машинного навчання можуть масштабуватися для ефективної обробки великих баз даних відбитків пальців. Вони можуть швидко й точно обробляти та порівнювати відбитки пальців із великою кількістю збережених записів.

2 АРХІТЕКТУРА НЕЙРОННИХ МЕРЕЖ

Будь-яка 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. 2.1).

Вхідний шар складається з вхідних нейронів, які передають інформацію в приховані шари. Прихований шар в свою чергу передає інформацію в вихідний. Кожен нейрон включає входи з вагами, що представляють собою синапси, функцію активації, визначальну вихідну інформацію в залежності від заданої вхідної, і один вихід. Синапси є регульованими параметрами, що перетворюють нейронну мережу в параметризовану систему.

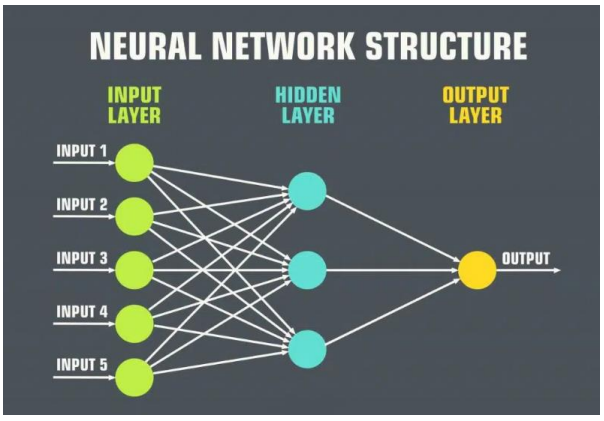

Рисунок 2.1 – Структура штучної нейронної мережі

Процес навчання (або тренування) у нейронних мережах включає оптимізацію ваг з метою мінімізації помилки передбачення, при цьому нейронна мережа досягає необхідного рівня точності. Найбільш поширеним методом для визначення внеску кожного нейрона в помилку є зворотнє поширення помилки, яке використовується для обчислення градієнту. Це є однією з модифікацій методу градієнтного спуску. Додавши додаткові приховані шари, можна зробити систему більш гнучкою і потужною. Нейронні

мережі з багатьма прихованими шарами отримали назву "глибокі нейронні мережі", і вони формують складні нелінійні зв'язки.

Нижче розглянемо декілька з популярних нейронних мереж, які себе добре показуть у сучасних нейролінгвістичних задачах і рекомендуються до використання.

2.1 Багатошаровий перцептрон

Багатошаровий перцептрон (Multilayer Perceptron, MLP) є типом штучного нейронного шару, який складається з кількох шарів нейронів, включаючи вхідний, приховані та вихідний [9]. Основна його особливість – наявність хоча б одного прихованого шару, що робить його більш гнучким та здатним до вивчення складних нелінійних залежностей в даних. Вхідний шар складається з нейронів, кількість яких рівна кількості вхідних ознак у вхідних даних. Кожен нейрон представляє собою вхідну ознаку. Приховані шари виконують обчислення та вивчають складні залежності між вхідним та вихідним шарами. Вихідний шар генерує вихід моделі.

Багатошаровий перцептрон (рис. 2.2) використовується для завдань класифікації та регресії в галузі машинного навчання. Навчання такого перцептрону здійснюється за допомогою методів оптимізації, таких як зворотнє поширення помилки, яке дозволяє адаптивно змінювати ваги для мінімізації помилок передбачення.

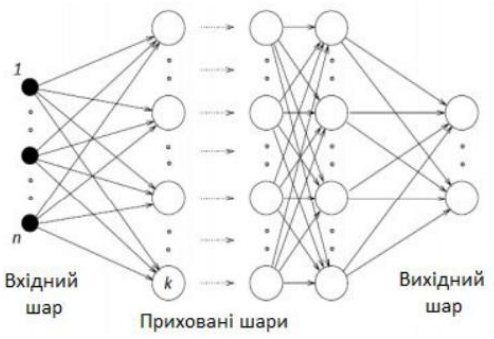

Рисунок 2.2 – Структура багатошарового персептрона

2.2 Рекурентна нейронна мережа

Рекурентна нейронна мережа (RNN) є типом штучного нейронного шару, який має здатність використовувати внутрішню пам'ять для обробки послідовних даних, таких як часові ряди, мовлення або текст. Одна з головних особливостей RNN – це наявність зв'язків між нейронами, які формують напрямлені цикли у графі обчислень, дозволяючи інформації передаватися через нейронні шари з попередніх моментів часу. У статті Natural Language Generation, Paraphrasing and Summarization of User Reviews with Recurrent Neural Networks (рис. 2.3) автори показують модель рекуррентной мережі, яка генерує нові пропозиції та короткий зміст текстового документа. Нейрони в RNN мають ваги, які визначають силу зв'язків між нейронами. Ці зв'язки формують напрямлені цикли в графі обчислень

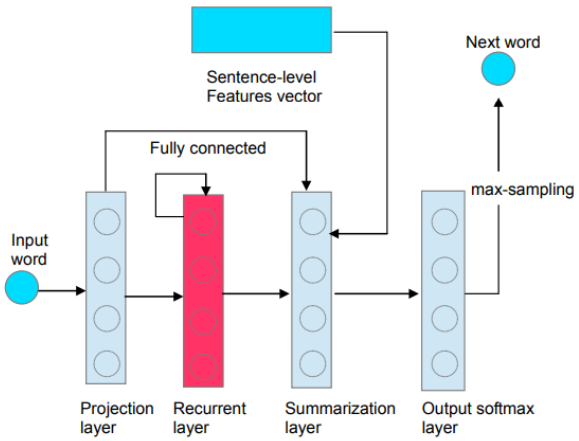

Рисунок 2.3 – Архітектура сумарної рекурентної нейронної мережі

Однак RNN мають обмежену здатність до ефективного навчання довгих залежностей через час (віддалені взаємодії у послідовних даних). Це призводить до виникнення проблеми "зниклого градієнта". У зв'язку з цим були розроблені модифікації RNN, такі як LSTM (Long Short-Term Memory) та GRU (Gated Recurrent Unit), які мають покращену здатність зберігати та використовувати інформацію на великому віддаленні в часі.

2.3 Мережа довгої короткострокової пам’яті LSTM

Long Short-Term Memory є розширенням рекурентної нейронної мережі (RNN) та була розроблена для подолання проблеми "зниклого градієнта" та покращення здатності моделі до роботи з довгими послідовностями даних. LSTM вперше була запропонована Хохрейтером та Шмідхубером у 1997 році. LSTM має механізм клітинного стану, який дозволяє нейронній мережі вибирати, що тримати та що забути із попередніх часових кроків. Також вона використовує функції активації, такі як сигмоїда та тангенс гіперболічний, для регулювання воріт та активації клітинного стану. Ця мережа здатна ефективно вирішувати проблеми зниклого градієнта та підтримує стабільну роботу з послідовностями тривалого періоду. Це робить її популярним вибором для різних завдань, таких як обробка мовлення, машинний переклад та генерація тексту [10].

2.4 Неглибокі нейронні мережі

Термін "неглибокі нейронні мережі" вказує на те, що це нейронні мережі з невеликою кількістю шарів, особливо в порівнянні з глибокими нейронними мережами, що складаються з багатьох шарів. Неглибокі мережі (рис. 2.4) можуть мати лише один або кілька прихованих шарів, у порівнянні з глибокими мережами, які можуть мати декілька десятків інтерпретаційних шарів. Основні характеристики неглибоких нейронних мереж:

– мінімальна а кількість шарів;

– обмежена абстракція;

– швидша тренування;

– можливі переваги в невеликих завданнях.

Неглибокі нейронні мережі можуть бути корисними у випадках, коли у вас обмежені обчислювальні ресурси, або коли завдання не вимагає глибокого розуміння вхідних даних. Однак для складних завдань, таких як розпізнавання

образів у великих наборах даних, глибокі нейронні мережі часто виявляються більш ефективними.

2.5 Згорткова нейронна мережа

Для розпізнавання людей за відбитками пальців або образами облич широко використовується архітектура нейронної мережі, відома як згорткова нейронна мережа (ЗНМ). Ця конкретна нейронна мережа була вперше описана в літературі і успішно використовується для вирішення різноманітних завдань, пов'язаних з розпізнаванням патернів. Такі завдання включають у себе розпізнавання тривимірних об'єктів, прогнозування погоди, автоматичне управління та інші [11].

Робота згорткової нейронної мережі базується на двох основних компонентах: фільтрах (визначниках ознак) та картах ознак. Фільтр представляє собою невелику матрицю, яка виділяє конкретну ознаку на вихідному зображенні. Наприклад, верхній фільтр визначає частини зображення з вертикальними лініями, а нижній – з горизонтальними.

Процес визначення базується на операції згортки фільтром оригінального зображення. Результати згортки, що визначають місцезнаходження ознак у вихідному зображенні, отримують назву карт ознак. Основна мета цього процесу – зменшити розмірність карт ознак до такого рівня, щоб мережа прямого поширення могла ефективно опрацьовувати їх повний набір.

Згортковий шар реалізує ідею локальних рецептивних полів, з'єднуючи кожен вихідний нейрон лише з обмеженою областю вхідної матриці. Це моделює деякі особливості людського зору.

Недоліки згорткових нейронних мереж включають високу складність архітектури, повнозв'язаність та фіксовану площу вікна шару згортки. Для підвищення ефективності роботи ЗНМ необхідно оптимізувати параметри,

такі як кількість карт ознак, щільність зв'язків між ними, розмір вікна, площа перекриття та початкова ініціалізація ваг.

2.5.1 Структура згорткової нейронної мережі

ЗНМ може складатися з різних видів шарів: згорткові, агрегувальні шари та шари «звичайної» нейронної мережі – персептрона. Модель такої мережі CNN можемо розглянути на рисунку 2.4.

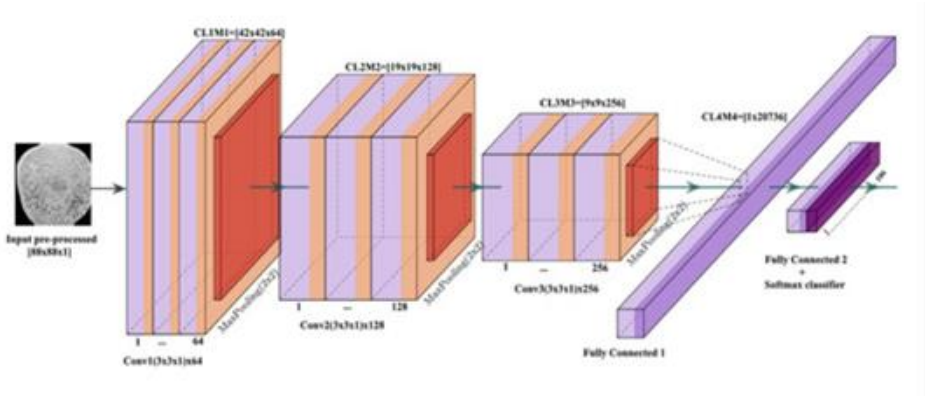

Рисунок 2.4 – Архітектура моделі CNN відбитків пальців

Перші два типи шарів, а саме згорткові та агрегаційні, взаємодіють між собою, утворюючи вхідний вектор ознак для багатошарового персептрона. Назва згорткових мереж виникла від операції згортання, суть якої буде розкрита надалі. Ці мережі представляють собою проміжний варіант між біологічними мережами та звичайним багатошаровим персептроном і на сьогоднішній день досягають найкращих результатів у обробці зображень. Середня точність розпізнавання за допомогою таких мереж перевищує звичайні нейронні мережі в середньому на 15%. Згорткові мережі є ключовою технологією глибокого навчання [12].

Основною причиною успіху згорткових нейронних мереж є концепція обмеженої кількості ваг. Незважаючи на великий розмір, ці мережі мають обмежену кількість змінних параметрів. Існують варіанти, такі як Tiled Convolutional Neural Network (TCNN), що схожі на неокогнітрон, де відбувається частковий показ взаємодії ваг, але алгоритм навчання

залишається незмінним і базується на основному методу зворотного розповсюдження помилок. Згорткові нейронні мережі можуть швидко функціонувати на спеціалізованих машинах та ефективно навчатись завдяки оптимізації процесів згортки на кожній карті ознак, а також зворотних згорток при передачі помилок через мережі.

Матриця ваг побудована так, що графічно кодує будь-яку ознаку, наприклад, наявність похилої лінії під певним кутом. Кожен шар, який виникає внаслідок операції згортки з відповідною матрицею ваг, вказує на наявність конкретної похилої лінії в оброблюваному шарі і визначає її координати, формуючи карту ознак. У сверточній нейронній мережі існує не один набір ваг, а ціла гама, яка кодує різноманітні лінії і дуги під різними кутами. Ядра згортки формуються самостійно в процесі навчання мережі методом звичайного розповсюдження помилок.

Операція субдискретізації (пулінгу) зменшує розмірність сформованих карт ознак. У цій архітектурі вважається, що інформація про наявність шуканої ознаки важливіша за точне визначення її координат. Тому вибирається максимальний нейрон з кількох сусідніх на карті ознак, і ця інформація приймається за один нейрон зменшеної розмірності. Іноді також застосовують операцію знаходження середнього значення між сусідніми нейронами, що робить мережу більш інваріантною до масштабу вхідного зображення.

Повторюючи кілька разів операції згортки і субдискретізації, будується згорткова нейронна мережа. Це дозволяє складати карти ознак і розпізнавати складні ієрархії ознак. Зазвичай, після кількох шарів, карта ознак стає вектором або навіть скаляром, але їх може бути сотні. На виході мережі додають декілька шарів перцептрона, на вхід якої подаються кінцеві карти ознак. Згортка часто використовується для обробки зображень і може бути описана наступною формулою:

$$(f \times g)\,[m,n] = \sum_{k,l} f\,[m-k,\ n-l] \times g[k,\ l], \tag{2.1}$$

де f – вихідна матриця зображення;

g – ядро (матриця) згортки.

На кожному кроці елементи вікна множаться елементами відповідних позицій ядра g, отримані значення підсумовуються, і результат записується в матрицю результату. Описана операція використовується в контексті згорткових нейронних мереж для визначення карт ознак на вхідних зображеннях.

Суть субдискретизації (рис. 2.5) та S-шарів полягає в зменшенні просторової розмірності зображення. Це означає, що вхідне зображення грубо (зазвичай шляхом усереднення) зменшується в задану кількість разів, частіше за все у 2 рази, але може бути і неоднаковий розмір зменшення, наприклад, в 2 рази по вертикалі та 3 рази по горизонталі.

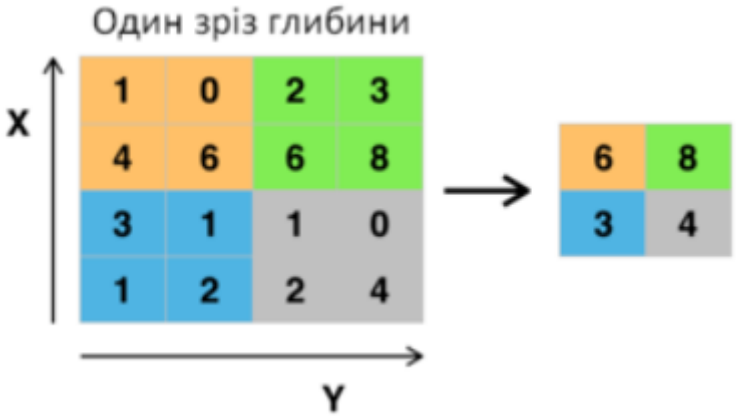

Рисунок 2.5 – Обробка країв згортки

Субдискретизація необхідна для забезпечення інваріантності до масштабу. Чергування шарів дозволяє складати карти ознак з карт ознак, що на практиці означає здатність розпізнавання складних ієрархій ознак. Зазвичай, після проходження декількох шарів, карта ознак перетворюється в вектор або навіть скаляр, але їх може бути сотні. У такому вигляді вони подаються на один-два шари повнонейронної мережі. Функції активації вихідного шару такої мережі можуть бути різні, від простої тангенціальної функції до використання радіальних базисних функцій.

2.5.2 Вхідний та згортоковий шари

Вхідний шар згорткової нейронної мережі виконує роль приймача вхідних даних, які можуть бути представлені у вигляді зображень. Кожен вхід цього шару може представляти інтенсивність пікселя або кольору в конкретній точці зображення. Головна особливість вхідного шару згорткової нейронної мережі полягає в тому, що він працює зі зображенням як цілісною структурою, зберігаючи просторову інформацію. Кожен нейрон в цьому шарі відповідає певній області (наприклад, пікселю або групі пікселів) вхідного зображення. Згорткові нейронні мережі використовують фільтри (ядра) для здійснення операції згортки на вхідних даних. Кожен фільтр визначає конкретну ознаку або патерн у зображенні. Під час операції згортки фільтр переміщується по всьому зображенні, взаємодіючи з різними частинами, та створює карту ознак, яка виділяє важливі характеристики.

Вхідний шар може також включати кілька каналів, які представляють різні аспекти або компоненти вхідних даних (наприклад, кольори у випадку RGB-зображень). Таким чином, вхідний шар забезпечує вхідні дані для подальшого аналізу та виявлення важливих ознак за допомогою подальших шарів згорткової нейронної мережі.

Згортковий шар, у свою чергу, що є ключовим будівельним блоком ОНР (основна нейронна мережа), має параметри, що включають в себе набір фільтрів, які призначені для навчання. Ці фільтри мають невеликі рецептивні поля, але простягаються на всю глибину вхідного об'єму. Під час прямого проходу кожен фільтр виконує згортку по ширині і висоті вхідного об'єму, розраховуючи скалярний добуток даних фільтра та вхідних даних. Цей процес формує двовимірну карту активації для кожного фільтра. В результаті навчання мережа визначає, які фільтри активуються при сприйнятті конкретного типу ознак у визначеному місці при вході. У більшості випадків пропонується брати співвідношення один до двух, якщо є карта попереднього шару, як вказано на рисунку 2.6. Взаємодія полягає у використанні ваг, які навчаються під час тренування мережі. Фільтри на поточному шарі

використовуються для здійснення згортки (кросс-кореляції) з картами ознак попереднього шару.

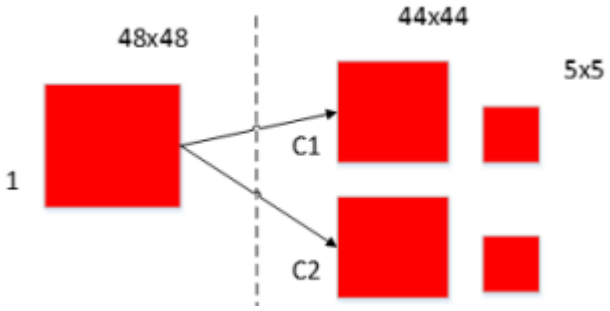

Рисунок 2.6 – Зв’язок між картами згонутого і попереднього шарів

Згортковий шар реалізує ідею – локальних рецептивних полів, тобто кожен вихідний нейрон з’єднаний тільки з невеликою областю вхідної матриці і таким чином моделює деякі особливості людського зору. У спрощеному вигляді цей шар можна описати формулою:

$$x^{\,l} = f(x^{\,l-1} * k^{\,l} + b^{\,l}), \tag{2.2}$$

де l – вихід шару l;

f () – функція активації;

b – коефіцієнт зсуву.

При цьому за рахунок крайових ефектів розмір вихідних матриць зменшується за формулою:

$$x_j^l = f(\sum_i x_i^{l-1} * k_j^l + b_j^l), \tag{2.3}$$

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

f () – функція активації;

bj – коефіцієнт зсуву для карти ознак j;

k_j – ядро згортки номер j;

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

Таким чином ядро визначає систему, у якій ваги розподілені. Це є однією з ключових характеристик згорткової нейромережі. У типовій багатошаровій мережі велика кількість зв’язків між нейронами, що призводить до наявності синапсів та в цілому замінює процес виявлення. У згортковій мережі, навпаки, загальна інформація дозволяє зменшити кількість зв’язків та забезпечити можливість виявлення тієї самої ознаки по всій області зображення.

2.5.3 Пулінговий та вихідний шари

Підвибірковий (пулінг) шар в згортковій нейронній мережі виконує операцію зменшення розмірності карт ознак, отриманих після згортки на попередньому шарі. Основна мета підвибіркового шару – зниження обсягу даних та підвищення інваріантності до малих трансформацій та змін у вхідних даних. Операція підвибіркового шару включає в себе взяття максимального (макс-пулінг) або середнього (середній пулінг) значення з певного регіону (зазвичай квадратного) на кожній карті ознак попереднього шару. Ця область пересувається по карті з певним кроком (строкою), що призводить до створення нової, зменшеної за розміром, карти ознак.

Підвибірковий шар допомагає вирізняти важливі ознаки та зменшує вплив невеликих змін у вхідних даних. Це також сприяє скороченню кількості параметрів у мережі, що допомагає уникнути перенавчання та прискорює обчислення. Загалом, підвибірковий шар є важливим елементом у структурі згорткових нейронних мереж, спрямованим на зменшення обчислювальної складності та підвищення працездатності мережі.

Також використовується процес регуляризації шарів при таких видах обчислень. Основна роль повнозв'язного шару полягає в об'єднанні та агрегації інформації, яку модель вивчила на попередніх шарах. Процес може бути здійснений різними методами, але найбільш поширеним є підхід застосування максимального пулінгу (рис. 2.7). У цьому випадку вся карта ознак

розбивається на області, з яких обирається елемент з максимальним значенням.

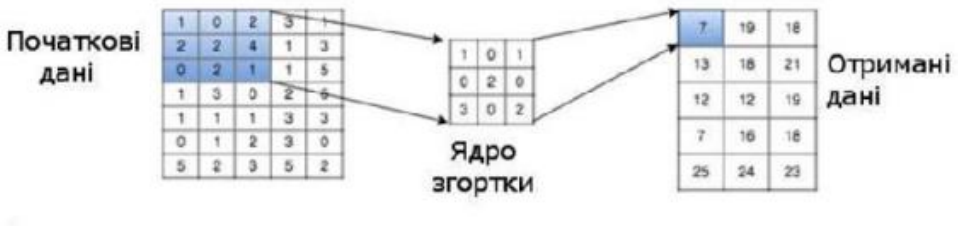

Рисунок 2.7 – Процес max-pulling

Вихідний шар взаємодіє з усіма нейронами попереднього шару. Кількість нейронів у цьому шарі відповідає кількості розподілених класів, а саме 2 класи: "об’єкт" та "не об'єкт". З метою скорочення кількості зв’язків та виконання обчислень для бінарного випадку можна використовувати один нейрон. При використанні гіперболічного тангенсу як функції активації, вихід нейрона зі значенням -1 вказує на приналежність до класу "не об'єкт", а значення 1 вказує на відповідність класу "об'єкт".

Розглянута згорткова нейронна мережа буде обрана для подальшого дослідження ідентифікації особи за відбитками пальця, з метою досягнення високої точності та надійності біометричної аутентифікації.

3 МЕТОДИ МАШИННОГО НАВЧАННЯ ТА РОЗПІЗНАВАННЯ ВІДБИТКІВ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Машинне навчання та штучний інтелект (ШІ) суттєво змінили сучасні методи ідентифікації особистості. Ці технології значно підвищили точність, ефективність і безпеку процесів ідентифікації в різних областях.

Однією з ключових сфер впливу є біометрична ідентифікація, яка включає розпізнавання відбитків пальців, розпізнавання обличчя, сканування райдужної оболонки ока, розпізнавання голосу та аналіз ходи. Машинне навчання та алгоритми ШІ підвищують точність і швидкість цих біометричних систем шляхом аналізу унікальних біологічних або поведінкових характеристик, що дозволяє точно ідентифікувати людей.

Програми для розпізнавання облич, наприклад, використовує алгоритми на основі ШІ для аналізу рис обличчя та шаблонів для ідентифікації людей. Ця технологія знаходить застосування в системах безпеки, правоохоронних органах, процесах автентифікації та контролі доступу, порівнюючи зроблені зображення з базою даних відомих облич. Ці системи точно ідентифікують людей на основі шаблонів, які використовуються в системах безпеки, віртуальних помічниках і програмах обслуговування клієнтів.

Системи розпізнавання відбитків пальця використовують алгоритми машинного навчання, які підвищують їх точність і швидкість. Автоматизовані системи порівнюють відбитки пальців із великими базами даних в області безпеки та криміналістики.

Аналіз поведінки на основі штучного інтелекту та машинного навчання вивчає поведінку в Інтернеті, наприклад, звички веб-перегляду та активність у соціальних мережах, щоб створити цифрові профілі для ідентифікації та аутентифікації.

Штучний інтелект сприяє створенню персоналізованих систем безпеки, адаптуючи заходи безпеки на основі індивідуальної поведінки та моделей.

Наприклад, аналіз шаблонів входу дозволяє використовувати адаптивні рівні аутентифікації, збалансовуючи безпеку та зручність роботи користувача. Це забезпечує високий рівень індивідуалізації у сфері безпеки, оскільки система може враховувати унікальні особливості та звички кожного користувача. Наприклад, якщо система виявляє незвичайність у зразках поведінки або входу, вона може взаємодіяти з користувачем, додатково підтверджуючи його особу або застосовуючи додаткові заходи безпеки.

У сфері виявлення та запобігання шахрайству машинне навчання та штучний інтелект відіграють вирішальну роль. Вони аналізують величезні масиви даних, виявляючи шаблони, що вказують на потенційне шахрайство, таким чином допомагаючи ідентифікувати та запобігати шахрайським діям, таким як викрадення особистих даних або захоплення облікових записів. Одним із дослідників цієї області є Крістіан Сегеді – комп’ютерний науковець і дослідник штучного інтелекту, відомий своїм внеском у глибоке навчання, зокрема різними досягненнями в архітектурі нейронних мереж, які вплинули на розпізнавання зображень і біометрію. Цей вчений разом з багатьма іншими дослідниками, продовжують розвивати технології ідентифікації особистості, зокрема в області біометрії. Їхній внесок має життєво важливе значення для підвищення точності, ефективності та етичних наслідків систем біометричної ідентифікації [13].

Однак збільшення використання штучного інтелекту для ідентифікації особистості викликає питання конфіденційності та етики. Важливо вирішити ці проблеми та забезпечити етичне використання цих технологій відповідно до нормативних актів для захисту прав і даних осіб.

Таким чином, машинне навчання та штучний інтелект зробили революцію в методах ідентифікації особистості, підвищивши точність, ефективність і адаптивність до потреб сучасного суспільства. Збалансування технологічних переваг із конфіденційністю, безпекою та етичними міркуваннями залишається критично важливим аспектом використання цих досягнень.

3.1 Основні типи машиного навчання

Машинне навчання відіграє вирішальну роль у розпізнаванні відбитків пальців, області біометричної аутентифікації. Можемо виділити декілька основних типів машинного навчання та те, як вони використовуються для розпізнавання відбитків пальця на основі штучного інтелекту (AI).

Контрольоване навчання широко використовується в розпізнаванні відбитків пальців для навчальних моделей для класифікації відбитків пальців на основі позначених навчальних даних. Модель вчиться розрізняти справжні та несправжні відбитки пальців. Приклади алгоритмів: опорні векторні мережі (SVM), k-найближчі сусіди (k-NN), нейронні мережі, дерева рішень.

Неконтрольоване навчання використовується для кластеризації та пошуку шаблонів у немаркованих даних відбитків пальців. Воно може ідентифікувати внутрішні структури та групувати відбитки пальців на основі схожості. Приклади алгоритмів: кластеризація K-середніх, ієрархічна кластеризація, аналіз головних компонентів (PCA).

Напівконтрольоване навчання використовується, коли існує обмежена кількість позначених даних і велика кількість не позначених даних. Це допомагає підвищити точність моделі, використовуючи обидва типи даних. Наприклад, це можуть бути алгоритми поєднання методів навчання під наглядом і без нагляду.

Навчання з підкріпленням рідше використовується в розпізнаванні відбитків пальців. Однак його можна використовувати в сценаріях, коли система взаємодіє з середовищем (наприклад, регулює якість зображення відбитків пальців) і отримує зворотний зв’язок для підвищення продуктивності з часом. Приклади алгоритмів: Q-Learning, Deep Q Networks (DQN), Proximal Policy Optimization (PPO) [14].

Глибоке навчання, підмножина машинного навчання, привернуло значну увагу та досягло успіху в розпізнаванні відбитків пальців. Згорткові нейронні мережі (CNN) та інші глибокі архітектури використовуються для

вилучення ознак і класифікації відбитків пальців. Приклади архітектур: згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN), мережі довготривалої короткочасної пам’яті (LSTM), сіамські мережі.

Навчання мережі використовується для покращення продуктивності моделей розпізнавання відбитків пальців шляхом використання попередньо навчених моделей для відповідних завдань. Потім ці попередньо навчені моделі можна налаштувати на основі даних відбитків пальців для підвищення точності та ефективності. Приклади підходів: точне налаштування попередньо навчених моделей CNN, таких як ResNet, VGG тощо, для вилучення функції відбитків пальців.

Розпізнавання відбитків пальців на основі штучного інтелекту в першу чергу передбачає виділення ознак, зіставлення та класифікацію. Моделі глибокого навчання, особливо CNN, показали виняткові перспективи в цій області, досягаючи найсучаснішої точності в задачах розпізнавання відбитків пальців. Моделі навчаються на великих наборах даних, що містять зображення відбитків пальців, щоб вивчати розрізнювальні функції та оптимізувати продуктивність розпізнавання.

3.2 Алгоритм роботи методів розпізнавання відбитків на основі штучного інтелекту

Сучасні методи розпізнавання відбитків пальців на основі штучного інтелекту використовують комплексні алгоритми та моделі машинного навчання для точного і надійного визначення особливих характеристик пальцевих відбитків. Постановка задачі будь-якої ідентифікації за допомогою ШІ полягає у наступному: виявлення дійсного користувача за допомогою порівняння з даними у базі даних за допомогою доступних методів ідентифікації, протидія шахрайству. Це завдання можна розділити на наступні кроки, зображені на рисунку 3.1.

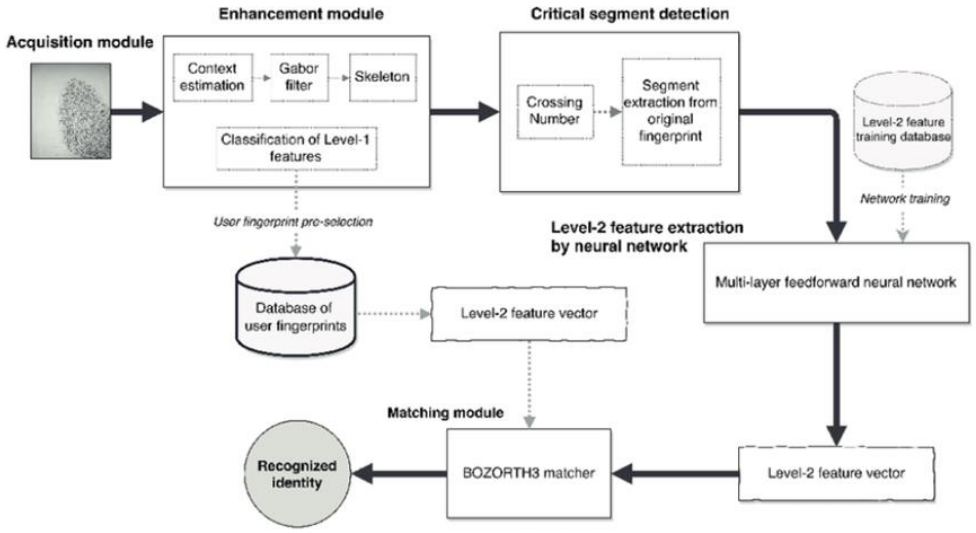

Рисунок 3.1 – Алгоритм виконання ідентифікації за допомогою AI

Виконання алгоритму починається з підготовки та попередньої обробки даних. Спершу відбиток пальця сканується для отримання зображення. Зображення піддається обробці для підвищення якості та зменшення шуму. Здійснення попередньої обробки біометричних зображень і проведення фільтрації можливе двома способами: вейвлет-Габором та вейвлет Ateb-Габором (рис. 3.2). Фільтр Габора на основі Ateb-функцій є ефективним для проведення фільтрації, оскільки містить узагальнення тригонометричних функцій [15].

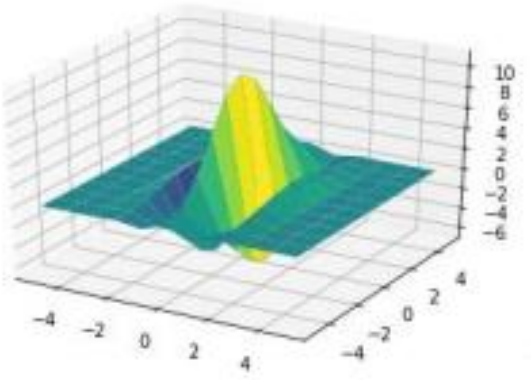

Рисунок 3.2 – Побудова вейвлет Габор фільтра з параметрами

Фільтрація та створення шаблону відбувається на основні методу особливих точок, такі як кінцеві точки та барабанні борозни, які є ключовими ознаками відбитків пальців. Особливі точки перетворюються на унікальний шаблон, що може бути представлений у числовому вигляді або у вигляді характеристичних векторів. Введення вейвлет перетворень дає змогу зменшити складність обчислень AtebGabor фільтра, спростивши обчислення функції та зменшивши час фільтрації. Фільтрування Ateb-Габором дозволяє змінювати інтенсивність всього зображення, та забезпечити зміну певних діапазонів, і таким чином змінити певні ділянки зображення. Якраз цю властивість мають біометричні зображення, на яких шаблони мають бути контрасними і чіткими. Ateb-функції мають властивість зміни двох раціональних параметрів, а це, в свою чергу, дасть можливість гнучкіше керувати фільтрацією. Досліджено властивості Ateb-функції, а також можливості зміни амплітуди функції, частоти коливань на чисельні значення фільтра Ateb-Габора. Завдяки використанню параметрів Ateb-функції можна отримати значно більший діапазон форм і величин, що розширює кількість можливих варіантів фільтрації. Також можна реалізувати один раз фільтрацію, врахувавши напрям вектору і надійно визначити чіткість країв, а не проводити фільтрацію багатократно.

Після створення шаблону відбувається безпосередньо використання алгоритмів машинного навчання, таких як нейронні мережі (зокрема, згорткові нейронні мережі), для навчання моделей розпізнавання та класифікації на основі створених шаблонів. Підхід до розпізнавання відбитків пальців полягає у вилученні векторів ознак з оригінальних зображень відбитків пальців за допомогою глибокого навчання безпосередньо.

Кінцевим загальним етапом ідентифікації за допомогою такого методу є визначення подібності та порівняння. Алгоритми порівняння оцінюють схожість між зразком відбитка пальця та збереженими шаблонами у базі даних.

На основі результатів порівняння приймається рішення щодо співпадіння або невідповідності відбитка пальця з вже збереженими шаблонами. Система вчиться та покращується з кожним новим зразком для підвищення точності та адаптації до змін у відбитках пальців.

У 2019 році Шервін Мінае та ін. застосував згорткову нейронну мережу для ідентифікації відбитків пальців. Він попередньо обробив оригінальний відбиток пальця зображення за допомогою традиційних методів обробки зображень, наприклад сушіння та фільтрування, після чого використовують Resnet-50 для витягнення векторів ознак і порівняння векторів [16]. Застосування архітектури Resnet-50 для витягнення векторів ознак свідчить про використання потужних глибоких нейронних мереж для аналізу складних особливостей відбитків пальців. Цей підхід дозволяє автоматично виділяти та вивчати характеристики, які можуть бути складні для виявлення за допомогою традиційних методів.

Глибоке навчання – це галузь машинного навчання, яка спеціалізується на використанні глибоких нейронних мереж, щоб аналізувати та враховувати складні структури в даних. Це означає, що можна використовувати нейронні мережі з багатьма шарами (глибокими архітектурами), щоб отримати краще розуміння та представлення даних. В контексті вирішення задач ідентифікації за відбитками пальців, глибоке навчання дозволяє створювати моделі, які автоматично вивчають значущі ознаки та шаблони у відбитках пальців. Ці моделі можуть розрізняти унікальні характеристики кожної особи, навіть у випадку близнюків, та ефективно використовувати ці ознаки для точної ідентифікації. Глибокі нейронні мережі можуть адаптуватися до надзвичайно складних та обширних даних, що є особливо важливим у випадку аналізу великих обсягів відбитків пальців.

Найпопулярніші методи глибокого навчання для вирішення завдань ідентифікації за відбитками пальців зазвичай включають використання різних типів нейронних мереж.

Наведемо приклади найбільш часто використовуваних нейронних мережевих архітектур і методів ідентифікації за відбитками пальців:

- згорткові нейронні мережі (CNN);
- сіамські нейронні мережі;
- повторювані нейронні мережі (RNN);
- капсульні мережі;
- мережі глибокої віри (DBN);
- автокодери;
- залишкові мережі (resnets);
- передача навчання.

Ці архітектури та методи нейронних мереж часто комбінуються або адаптуються відповідно до конкретних вимог і складності завдань ідентифікації за відбитками пальців. Експериментування та налаштування на основі набору даних і наявної проблеми мають вирішальне значення для досягнення оптимальних результатів [17].

Згорткові нейронні мережі (CNN) є ефективними для розпізнавання відбитків пальців через їхню здатність ефективно аналізувати зображення. Для створення системи розпізнавання відбитків пальців з використанням CNN, слід виконати кілька кроків:

1) зібрати велику кількість відбитків пальців у форматі зображень. Ці зображення потрібно обробити, вирізавши та нормалізуючи їх, щоб підготувати для використання у нейронній мережі;

2) створити архітектуру CNN, яка складатиметься зі згорткових шарів, пулінгових шарів, повнозв'язних шарів та функцій активації. Оптимальну архітектуру можна визначити експериментально;

3) використати навчальні дані для навчання моделі. Введіть дані у мережу та скоригуйте ваги так, щоб модель навчилася розпізнавати відбитки пальців;

4) розбити дані на навчальні та тестові набори. Протестуйте модель на тестових даних та оцініть її точність та ефективність;

5) оптимізувати модель, вдосконалюючи архітектуру та параметри для отримання кращих результатів.

3.2.1 Адаптивна модель CNN

Основною складовою моделі CNN є згортковий (CONV) шар. Він виділяє дискримінаційні характеристики з вхідного сигналу, застосовуючи операцію згортки з фільтрами фіксованого розміру. Шари CONV складаються в моделі CNN для вилучення ієрархії функцій. Кількість фільтрів у кожному шарі CONV і кількість шарів CONV у моделі CNN є гіперпараметрами, і пошук найкращої конфігурації моделі для конкретного застосування є важкою проблемою оптимізації. Це тягне за собою пошук величезного простору параметрів. Крім того, ініціалізація параметрів моделі CNN, які можна вивчати, має значний вплив на продуктивність моделі, коли вона навчається за основі ітераційного алгоритму оптимізації, такого як оптимізатор Адама.

Використовуючи дискримінаційний вміст відбитків пальців, пропонується простий метод адаптивного пошуку найкращої конфігурації моделі. Спочатку модель відбирає репрезентативні відбитки пальців для кожного типу, щоб керувати процесом розробки моделі CNN. Дискримінаційна інформація в цих відбитках використовується для визначення ширини (кількості фільтрів) кожного шару CONV і глибини (кількості шарів CONV) моделі. В цьому випадку використовується кластеризація для вибору репрезентативних відбитків пальців, перетворення Фукунаги-Кунца (FKT), яке використовує дискримінаційну інформацію про класи, щоб визначити кількість фільтрів у шарі CONV та співвідношення міжкласової матриці розсіювання S_b до матриці розсіювання всередині класу S_w для налаштування глибини (тобто кількості шарів CONV) моделі CNN. Щоб мінімізувати кількість параметрів, які можна вивчати, і уникнути переобладнання, вводяться рівні глобального об’єднання. Зменшуючи роздільну здатність карт

функцій, шар об’єднання прагне досягти інваріантності зсуву, а карта функцій рівня об’єднання пов’язана безпосередньо з SoftMax.

3.2.2 Архітектура DeepFKTNet

Первинна архітектура DeepFKTNet базується на відповідях на два запитання: скільки шарів CONV має бути в моделі та скільки фільтрів має бути в кожному шарі. Ці питання вирішуються за допомогою ітераційного алгоритму, який обчислює кількість фільтрів у шарі CONV, ітеративно додає його до моделі та завершує роботу, коли критерій задовольняється. Ми використовуємо дискримінаційну структурну інформацію, вбудовану в відбитки пальців, щоб визначити кількість фільтрів у шарі CONV та їх ініціалізацію. Щоб зменшити розмір карт функцій для ефективності обчислень, шари об’єднання додаються після першого та другого блоків CONV. Оскільки ядра та їх кількість визначаються із зображень відбитків пальців, кожен шар може мати різну кількість фільтрів. Модель DeepFKTNet оцінюється за допомогою тестового мультисенсорного набору даних FingerPass і порівнюється з добре відомими глибинними моделями: ResNet і DenseNet, попередньо навченими на наборі даних ImageNet і налаштованими за допомогою того самого набір даних як DeepFKTNet.

За допомогою моделі DeepFKTNet можна розробити систему для кожного набору даних і налаштувати її за допомогою навчальних наборів. Просторова складність моделі CNN вимірюється кількістю параметрів, які можна вивчати, тоді як кількість FLOPS визначає її часову складність.

Загалом моделі CNN містять велику кількість параметрів і розроблені випадковим чином, таким чином можна використовувати підхід FKT для створення недорогої високошвидкісної моделі CNN, адаптованої для цільового набору даних відбитків пальців. У порівнянні з найсучаснішими методами на наборі даних FVC2004, модель DeepFKTNet-5 простіша з точки зору складності та кількості параметрів і досягає порівнянної продуктивності.

3.3 Сіамські нейронні мережі

Розпізнавання відбитків пальців є найпоширенішим методом ідентифікації в даний час. Однак він все ще не вистачає з точки зору кросплатформності та алгоритмічної складності, що певним чином впливає на міграцію даних відбитків пальців в суцільну базу і розвиток системи. Запропонований у цьому дослідженні метод надає змогу вбудованим алгоритмам обробки зображень на основі сіамської нейронної мережі в методі розпізнавання, розпізнавати зображення з будь-якого джерела без попереднього створення бази даних для зберігання зображень. Результати показали, що точність запропонованого алгоритму склала до 92%, а його оцінка F1 – до 0,87.

Згорткова нейронна мережа (CNN) є найпоширенішим методом обробки зображень. Сіамська нейоронна мережа, як розширений метод CNN є зв’язаною структурою, встановленою між двома штучними нейронними мережами. Після того, як два зображення надходять у CNN і порівняльну мережу з функцією втрат, виводиться релевантність між зображеннями [18]. Всі бінарні зображення відбитків пальців були введені в сіамську нейронну мережу, щоб отримати подібність між двома відбитками пальців і отримати результат розпізнавання відбитків пальців. Вся система потребувала виконання таких етапів, як стандартизація зображення відбитків пальців, покращення зображення, бінаризація, введення в сіамську мережу та виведення результату відповідності.

Зображення відбитків пальців, отримані під час збирання відбитків пальців, мали наступні чотири дефекти:

– різні сили натискання та напрямки пальців можуть призвести до зміни відтінку зображення відбитків пальців;

– різні рівні сухості та вологості пальців можуть зробити зображення відбитків пальців занадто сухими або надто вологими та не мали відповідних характеристик;

– зображення відбитків пальців було переривчастим через зморшки та шрами на пальцях.

На зібраному зображенні були нерегулярні шуми або плями. Попередня обробка зображень відбитків пальців – це технологія, яка може покращити якість зображень відбитків пальців, а зображення відбитків пальців, оброблені за допомогою цієї технології, можна краще обробляти пізніше.

Зображення відбитків пальців стандартизовано, щоб усунути проблеми непостійної чіткості, відтінків сірого та кількості каналів між різними зображеннями відбитків пальців.

Припускаючи, що значення сірого у вихідному зображенні було сірим (x, y), а розмір зображення становив M×N, можна отримати середнє значення сірого (mean) і дисперсію сірого (var). Метод розрахунку такий:

$$mean = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} gray\big(i + x * Mj + y * N\big),$$

$$var = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [gray(i+x*M, j+y\times N) - mean}{M*N},$$

де $L_{i,j}$ – відстань між векторами ознак;

M, N – карти ознак попереднього шару.

x – коефіцієнт зсуву.

Платформа Deep Learning Framework дозволяє оцінити, чи належать дві записані поведінки одному користувачу. Цей підхід може автентифікувати користувача лише після одного спостереження (тобто поведінки реєстрації). SOS-NN обчислює подібність між двома вхідними даними поведінки. У цьому сенсі, якщо є два входи досить схожі, наша система робить висновок, що вхідна поведінка належить законному користувачеві. Архітектура сіамської мережі складається з двох ідентичних підмереж. У випадку оцінення цим

методом є дві повністю з'єднані нейронні мережі, які ділять ваги. Кожна підмережа обробляє одну з вхідних дій і працює як екстрактор функцій.

Обидва виходи підмережі обмежені функцією енергії. Ми обчислюємо відстань L_i, як енергетичну функцію між обома обчисленими векторами ознак у латентному просторі. Інтуїтивно, ця відстань має бути великою, якщо поведінка введення належить різним користувачам, але малою, коли вони належать одному користувачеві. Після розрахунку функції енергії можна включити в модель повністю пов’язана мережі прийняття рішень, яка приймає рішення щодо класифікації на основі відстані між векторами ознак у латентному просторі. Отже, вихід SOS-NN є двійковим класифікатором, де результатом є одиниця, якщо поведінка належить тому самому користувачу, і нуль в іншому випадку (рис. 3.3).

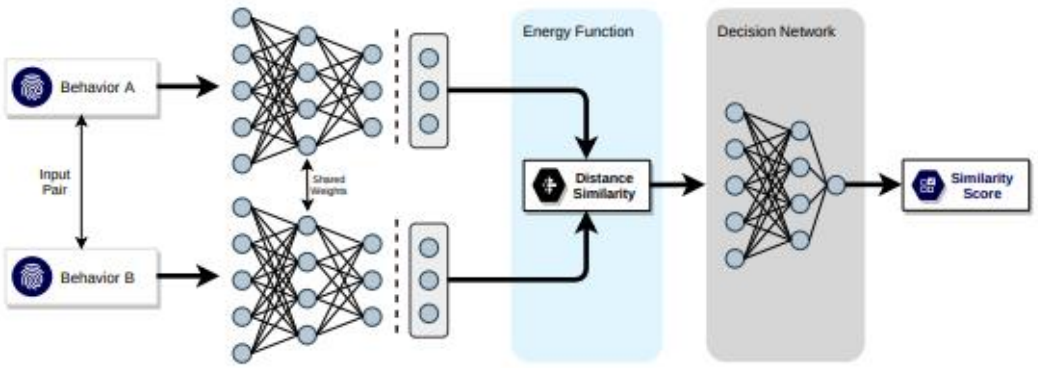

Рисунок 3.3 – Приклад архітектури SOS-NN

Сіамські мережі вчаться, порівнюючи пари поведінки. Позитивна пара визначається як пара двох поведінок, які належать одному користувачеві, тоді як пара поведінок різних користувачів позначається як негативна пара. Модель навчається шляхом представлення кількох таких зразків.

Метою навчання є мінімізація енергетичної функції (тобто відстані L_1) між поведінками в позитивних пар і максимізувати енергетичну функцію для негативних пар. Звичайний відбір тих позитивних і негативні пар є випадковим вибором. Цей підхід підходить для позитивних пар, але для

негативних зразків дуже важливо вибрати високоякісні пари. Можна використовувати більш просунуті методи для вибору навчальних зразків, як-от техніка триплетних втрат, яка використовує одночасно 3 приклади оптимізування кожного кроку навчання.

Процедура навчання залежить від стратегії формування вибірки (звичайна чи триплетна). Для звичайної парної стратегії, ми навчаємо наш SOS-NN, використовуючи перехресну втрату ентропійної мети на нашому двійковому класифікаторі (однокові або різні користувачі). Тому для звичайної стратегії ми виконуємо оптимізацію ваг над повною мережею (включаючи сіамську мережу та мережу рішень), використовуючи стандартне зворотне поширення. Градієнт є адитивним для пов'язаних підмереж. З іншого боку, для стратегії триплету навчання проводиться в два етапи: навчання сіамської мережі та навчання рівня прийняття рішень. Для навчання сіамської мережі, використовується конфігурація Semi-Hard Triplets. Екстрактор функцій та їх ваги стандартизуються, а повністю пов'язаний рівень прийняття рішень додається для завершення SOS-NN. Після цього відбувається процес навчання прийняття рішень, використовуючи двійкову крос-ентропію як функцію втрат.

У цьому дослідженні використовувалася платформа PyTorch для побудови основної мережі, а канал вхідного рівня був встановлений на 128×128×3. Дві основні мережі були експортовані до функції втрат.

Функція втрат, використана в цьому дослідженні, була контрастною втратою. Цей тип функції втрат був ефективним у обробці зв'язку між виходами двох основних мереж у сіамській мережі. Його мінімальна відстань втрати становить:

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

Векторна відстань L , яка була виведена, була повністю пов'язана двічі

після обчислення функції втрат, а вихідний рівень прийняв сигмоподібну функцію для нормалізації отриманих значень. Мережа в цьому сегменті була мережею порівняння. Якщо релевантність між двома зображеннями була високою, вихідні дані зміщувалися до 1. В іншому випадку вихідні дані зміщувалися до 0.

У цьому дослідженні ми навчили наведену вище сіамську мережу за допомогою 8 різних відбитків пальців і використовували зображення відбитків пальців розміром 128×128. Зображення відбитків пальців того самого пальця в навчальному наборі зберігалися в одній папці. Для основної мережі VGG попередньо навчені мережеві ваги VGG16 використовувалися для наступного навчання мережі в цьому дослідженні.

У навчальному наборі є 4 види зображень відбитків пальців, які належать різним пальцям, зібраних пристроєм-збирачем відбитків пальців AS60x. Для кожного з різних відбитків пальців у навчальному наборі було відібрано в середньому 3 зображення (рис. 3.4). Усі зображення в навчальному наборі пройшли попередню обробку відбитків пальців, як описано вище. З метою підвищення адаптивності навчального набору та навчання кожне зображення відбитка пальця оберталося п’ять разів, і загалом було отримано три зображення. Завдяки такому навчанню операцій кількість зображень кожного відбитка пальця зросла в середньому до 6.

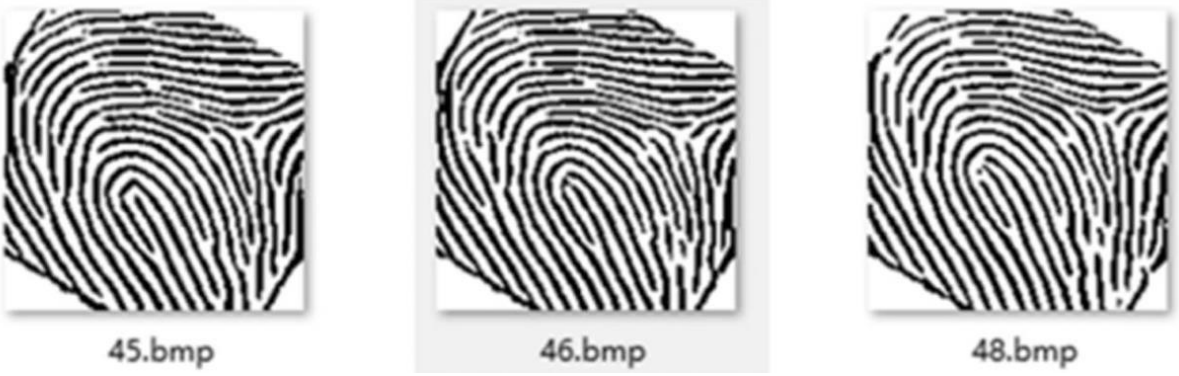

Рисунок 3.4 – Навчальний набір з трьох зображень розміром 128 × 128

Стосовно навчання порівняльної мережі, два зображення одного виду були взяті з навчального набору, і вихід був відкалібрований до 1. Зображення іншого типу було вилучено, і вихід був відкалібрований до 0, разом із зображення в перших двох розділах. Інше зображення іншого типу було вилучено, попередній крок продовжено, а набір даних відкалібровано. Після навчання таким чином, коли було введено два зображення відбитків одного пальця, мережевий вихід був зміщений до 1. В іншому випадку, мережевий вхід змішувався до 0.

Параметри та результати навчання використовуються таким чином:

– розмір партії дорівнює 32;

– швидкість навчання дорівнює 0,001;

– епоха дорівнює 1000;

– загальні втрати дорівнює 0,1149;

– тривалість навчання – 3 дні;

– тестовий час на період – 600 мс.

Звичайний алгоритм Гальтона був застосований до бази даних попередньої обробки зображень, запропонованої в цьому дослідженні. Результати показали, що запропонована база даних була сумісною зі звичайною системою, і цільову систему було успішно створено.

У цьому дослідженні пропонується метод зіставлення зображень на основі вбудованої сіамської нейронної мережі та застосовується до зіставлення відбитків пальців, який може виконувати розпізнавання відбитків пальців із будь-яких джерел (баз даних, фотографій і зображень) за допомогою вбудованого алгоритму обробки зображень, тому що етапи створення бази даних зображень відбитків пальців можна опустити.

У порівнянні зі звичайними методоми розпізнавання відбитків пальців, які вимагають виділення дрібниць і відповідного зіставлення, дослідження на основі сіамської нейромережі ідентифікує відбитки шляхом безпосереднього використання методу порівняння зображень відбитків пальців із сіамською нейронною мережею та подальшого виведення значення подібності.

4 КОМП'ЮТЕРНА МОДЕЛЬ РОЗПІЗНАВАННЯ ВІДБИТКІВ ПАЛЬЦЯ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

4.1 Вибір програмних комплексів для поставлених задач

У даній кваліфікаційній роботі для розробки та реалізації методу ідентифікації відбитків пальців на основі нейроних мереж з використанням CNN було обрано наступні програмні засоби: Python, MatLab з комплексом Residual Network 50, Android Studio Java.

4.1.1 MatLab та Deep Learning Toolbox

Програмне забезпечення для нейромереж використовується для створення, вивчення, розробки та застосування штучних нейронних мереж, штучного інтелекту і технологій машинного навчання. У рамках кваліфікаційної роботи для реалізації поставлених задач обрано програмний засіб MatLab. Це одна з інноваційних систем для автоматизації математичних обчислень, що базується на розширеному використанні матричних операцій. Використання матриць широко розповсюджене в складних математичних розрахунках, таких як розв'язання завдань лінійної алгебри і математичного моделювання статичних та динамічних систем і об'єктів. Matlab має багато спеціалізованих інструментів для різних галузей, таких як обробка сигналів, обробка зображень, машинне навчання, статистика, оптимізація та інші.

Matlab може взаємодіяти з іншими мовами програмування, такими як C, C++, Java, Python, що дозволяє використовувати його як частину складних програмних систем. Його засоби дозволяють розгортати треновані моделі для використання в реальних застосунках, наприклад, у вбудованих системах або в середовищах виробництва. Він підтримує паралельні обчислення, що дозволяє використовувати потужності багатьох ядер процесора для прискорення обчислень, зокрема у тренуванні великих моделей.

Також цей комплекст використовується для розробки, тренування та експериментів з нейронними мережами через використання вбудованих інструментів та бібліотек для глибокого навчання. Наприклад, такі інструменти, як Deep Learning Toolbox, Simulink, Signal Processing Toolbox та інші.

Таким чином, використання Deep Learning Toolbox дозволяє використовувати функції для створення, тренування та валідації глибоких нейронних мереж. Включає в себе підтримку згорткових мереж (CNN), рекурентних мереж (RNN), а також можливості для передачі навчання та використання попередньо навчених моделей. Цей інструмент надає широкий спектр функцій тренування, які дозволяють налаштовувати параметри тренування, вибирати оптимізатори, функції втрат та інші параметри. Містить функції для відображення архітектур мережі, відстеження кривих навчання та візуалізації ваг моделі. Деякі функції Deep Learning Toolbox підтримують спеціалізовані апаратні засоби, такі як FPGA (Field-Programmable Gate Array), для прискорення виконання деяких операцій. Deep Learning Toolbox відкриває широкі можливості для дослідження та розробки глибоких нейронних мереж в середовищі MATLAB.

4.1.2 Python

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, та PyTorch, який є найбільш популярними. Крім того, бібліотека Keras, яка інтегрується з TensorFlow, надає високорівневий інтерфейс для швидкої розробки нейронних мереж. У сфері обробки зображень Python використовується з бібліотеками, такими як OpenCV та Pillow. Також важливою є підтримка графічних процесорів для

прискорення обчислень у нейромережах, і це реалізується через TensorFlow та PyTorch.

Усі ці аспекти роблять Python зручним та популярним вибором для розробки та дослідження нейромереж, завдяки його простоті та широким можливостям.

4.1.3 ResNet-50

ResNet-50 (Residual Network із 50 шарами) є архітектурою глибокої згорткової нейронної мережі, яку представило Microsoft Research у роботі під назвою "Глибоке залишкове навчання для розпізнавання зображень" Каймінг Хе, Сянгю Чжан, Шаочінг Жен і Джіан Сун. Ця модель була представлена на конференції з комп'ютерного зору та обробки зображень у 2016 році (CVPR). Це глибока нейромережа з архітектурою, що використовує "залишкові блоки" (residual blocks), які дозволяють досить ефективно тренувати глибокі мережі.

Традиційні глибокі мережі стикаються з проблемою зниклих або вибухаючих градієнтів, що ускладнює тренування глибоких моделей. Залишкове навчання вирішує цю проблему за допомогою з'єднань скорочення (skip connections), що дозволяють прокладати інформаційний потік безпосередньо від одного шару до іншого. Вона використовує бутельові структури в своїй архітектурі, які використовують згортки 1x1, 3x3 та 1x1 для зменшення обчислювальної складності при збереженні представлення. З'єднання скорочення дозволяють градієнту легко протікати під час зворотного розповсюдження, вирішуючи проблему зникання градієнту.

Зазвичай ResNet-50 використовує глобальне середнє згладжування замість традиційно повних з'єднаних шарів в кінці мережі. GAP зменшує просторові розміри карт ознак до одного значення для кожної карти ознак, отримуючи компактне представлення.

Цю архітектуру широко використовують у завданнях комп’ютерного зору, класифікації зображень, виявлення об’єктів та сегментації.

4.2 Реалізація CNN для розпізнавання відбитків пальця

Застосування розпізнавання відбитків пальців за допомогою нейронних мереж має великий потенціал і вже знаходить широке застосування у різних сферах життя. Наприклад, в такій сфері як безпека, кримінальне слідство та кібербезпека застосовуються аспекти таких систем для біометричної ідентифікації осіб. Застосування нейронних мереж дозволяє створити ефективні та точні системи ідентифікації осіб, що можуть допомагати в розслідуванні злочинів та запобіганні несанкціонованому доступу. Також такі системи знахоодять місце для аутентифікації користувачів в різних сферах, таких як мобільні пристрої, банківські системи та інтернет-платформи. Застосування нейронних мереж у цьому контексті допомагає зробити системи більш надійними та відповідними.

Якщо говорити про впровадження нейроних мереж у системи доступу до фізичних об’єктів, розпізнавання відбитків пальців може бути використано для контролю доступу до будівель, офісів, складів та інших об'єктів. Автоматизовані системи, побудовані на нейромережах, можуть спростити процес надання послуг і забезпечити конфіденційність та надійність.

Тож, реалізована комп’ютерна модель є актуальною у багатьох сферах ідентифікації доступу та у подальшому може бути розширена та удосконалена для більших масивів даних і для різних підходів навчання мереж.

Для навчання нейромережі був використаний датасет, що складався з 4000 фотографій відбитків пальців у форматі PNG (рис. 4.1). Робоча область проекту була визначена за адресою C:\MatLab на локальному комп’ютері. Важливим етапом перед самим процесом навчання є підготовка даних. Навіть при наявності коду для пре-підготовки, важливо, щоб дані мали однаковий розмір. У даному випадку, враховуючи, що об'єктами є відбитки пальців, вирішено перетворити всі кольорові фотографії у чорно-білі, що дозволяє досягти більшої лаконічності коду та уникнути проблем з форматом. Варто зазначити, що важливо застосувати підходи для зменшення кількості

обмежувальних контурів в тренувальному наборі. Це допоможемо у вирішенні проблем, таких як перенавчання (overfitting) та підвищення обсягу даних.

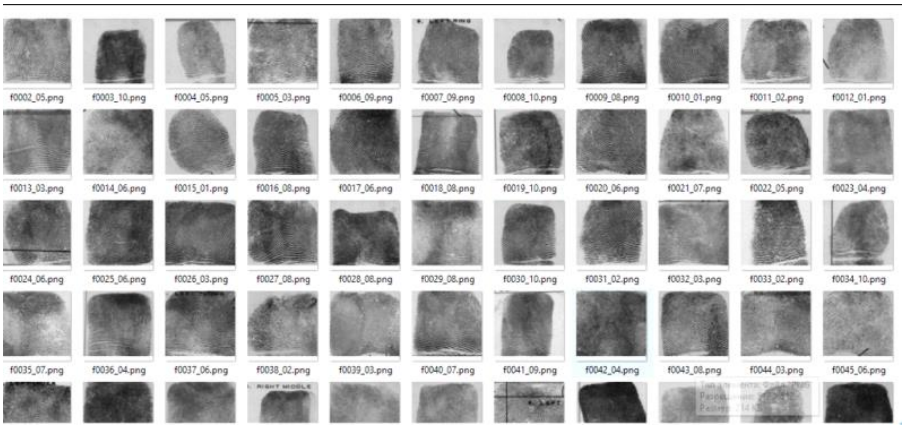

Рисунок 4.1 – Датасет відбитків пальців у форматі .png

Розміри фотографій в оригінальному датасеті різняться, тому їх потрібно попередньо обробити. У даному випадку був використаний Python-скрипт для масштабування зображень до єдиної розмірності 224x224. Крім того, скрипт (лістинг 4.1) перетворює кольорові фотографії в чорно-білі, а фінальний формат зображень стає 224x224x3. Змінені фотографії зберігаються у робочій директорії в окремій папці ResizeDataset, цей підхід дозволяє стандартизувати формат та розміри зображень перед подальшим використанням їх для навчання нейромережі.

Лістинг 4.1 – Функція попередньої обробки зображень

```
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;
```

4.3 Алгоритм роботи програми

Можемо виділити наступні кроки в алгоритмі роботи розробленої моделі:

1) попередня обробка даних: зображення відбитків пальців завантажуються та піддаються попередній обробці для покращення якості та чіткості, застосовується алгоритм виявлення контурів за допомогою алгоритму Canny для виділення ключових особливостей;

2) підготовка наборів даних: дані розділяються на навчальний і тестовий набори для ефективного тренування та оцінки моделі, зображення зберігаються в нових директоріях після попередньої обробки для подальшої роботи з ними;

3) створення згорткової нейромережі: архітектура нейромережі, яка включає в себе шар входу, згорткові шари для вилучення рис та особливостей, ReLU-шари для активації та покращення нелінійних властивостей, та шар класифікації для кінцевого результату;

4) налаштування та тренування нейронної мережі: визначаються параметри тренування, такі як кількість епох, розмір пакету (batch size), функція втрат для визначення помилок та оптимізатор для корекції ваг нейромережі, нейромережа тренується на навчальному наборі для вивчення ключових особливостей та шаблонів відбитків пальців;

5) тестування та оцінка: тестовий набір використовується для перевірки точності та ефективності моделі, обчислюється точність класифікації, яка вказує, наскільки добре модель розпізнає відбитки пальців на нових зображеннях;

6) пошук схожих відбитків пальців: навчена модель для класифікації нового зображення відбитку пальця, виводиться результат класифікації, що може вказувати на ідентифікацію конкретного відбитку або його відмінність від вже відомих шаблонів.

Цей алгоритм поєднує в собі різні етапи обробки даних, підготовки наборів, створення та налаштування нейромережі та тестування для розпізнавання відбитків пальців, що робить його повноцінним та комплексним підходом до задачі біометричної ідентифікації.

4.4 Використання методів для виявлення контурів, морфологічні операції, 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 описані в лістингу 4.2.

Лістинг 4.2 – Виявлення та розширення контурів за допомогою морфологічних операцій

```
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');
```

Ця функція 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. 4.2).

Науковий підхід цієї функції полягає у використанні алгоритму Canny для виявлення контурів, що дозволяє вирізати фон та ізолювати основний об'єкт інтересу. Завдяки цьому, вона виявляє робочу область на фотографії, що містить відбиток пальця.

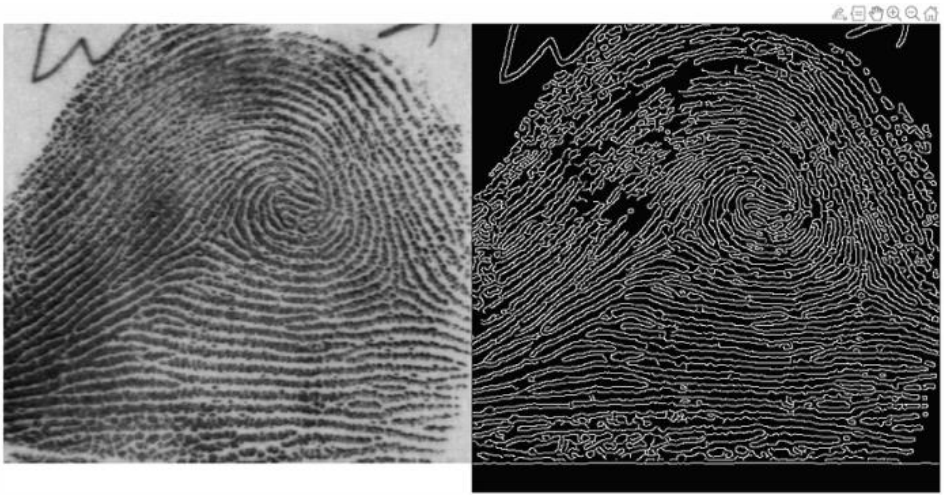

Рисунок 4.2 – Візуалізація роботи функції для виділення ознак

Щодо функції розширення контурів на основі морфологічних операцій – цей процес надає можливість виділяти ключові структурні елементи відбитка, що допомагає в підготовці даних для подальшого аналізу. Іншими словами, функція виступає куратором, який керує та обирає лише найсуттєвіше зображення відбитка пальця для подальших обчислень та аналізу високорівневих ознак.

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. Він вирізняється високою ефективністю та швидкістю обчислень, що робить його відмінним вибором

для задач реального часу та великих обсягів даних. Приклад роботи алгоритму зображено на рисунку 4.3.

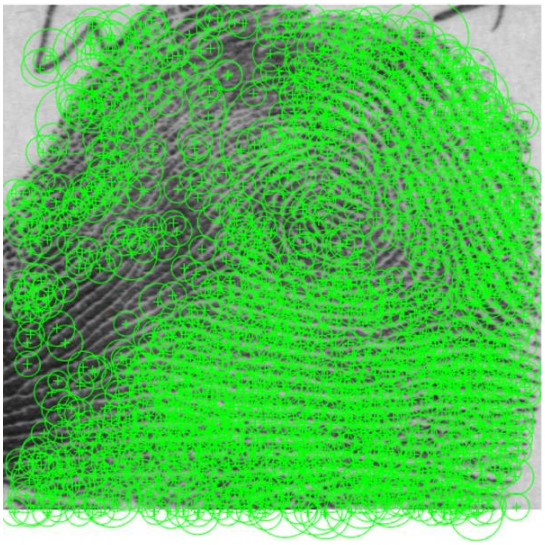

Рисунок 4.3 – Візуалізація виявлення важливих точок відбитку із датасету

4.5 Навчання нейронної мережі

Умови і параметри навчання задані в коді програми. Після закінчення навчання модель зберігається в робочу область проекту. На рисунку 4.4 зображено графік навчання, в якому представлені наступні дані та результати навчання: Loss, Validation Loss, Accuracy.

Loss (втрати) представляє собою метрику, що визначає, наскільки точно нейромережа робить прогнози під час навчання. Основна мета полягає в тому, щоб мінімізувати цю величину протягом ітерацій навчання, щоб модель набула найкращих можливих здатностей передбачення.

Validation Loss (втрати на валідації) є величиною втрат, оціненою на окремому наборі даних, який не брав участь у навчанні моделі. Ця метрика використовується для об'єктивної оцінки ефективності мережі на даних, які вона раніше не "бачила", що допомагає виявити ознаки перенавчання та загальну адаптованість моделі.

Accuracy (точність) представляє собою відношення правильних прогнозів до загальної кількості прогнозів. В межах навчання мережі, мета полягає в збільшенні точності для кращого відтворення реальних патернів та закономірностей у навчальних даних.

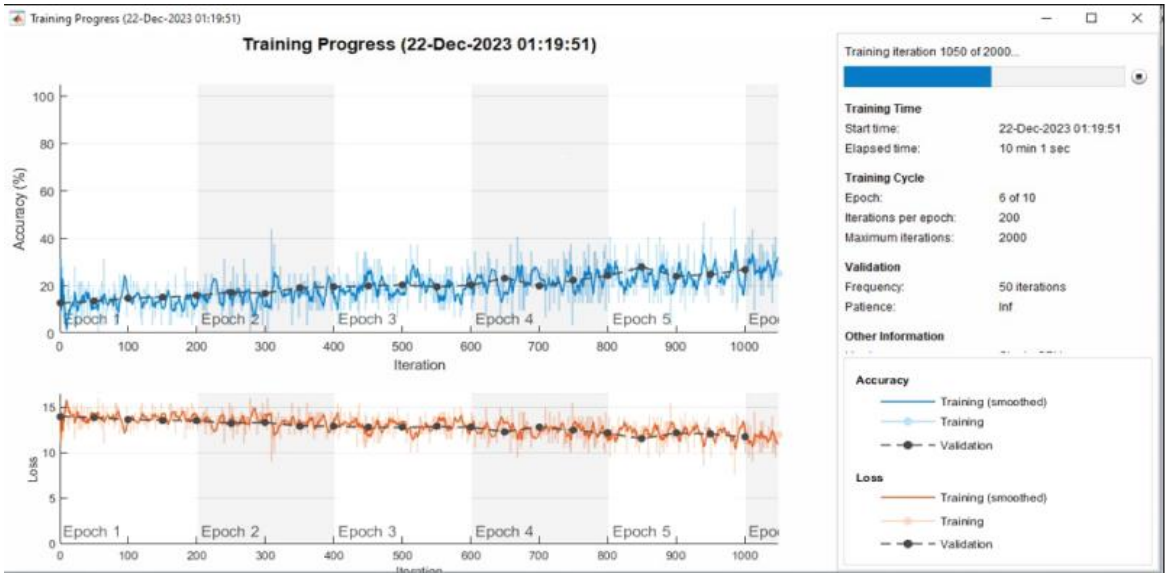

Рисунок 4.4 – Графік навчання нейромережі

Графіки, які візуалізують ці метрики протягом ітерацій навчання, надають можливість кращого розуміння ефективності моделі. Зниження втрат та збільшення точності на тренувальному та валідаційному наборах може вказувати на успішне навчання. Інтерпретація графіків вимагає уважності та контекстуального розуміння конкретної задачі та даних, оскільки можуть існувати сценарії перенавчання або недостатньої узагальненості моделі. Після навчання нейромережі запускаємо «перенавчання». Тобто, навчання по тому ж датасету, щоб перевірити наскільки точно мережа запам’ятала зображення. Вивід результату показує 100% точність навіть для першої епохи навчання.

4.6 Результат розробленої моделі та практичне застосування

У результаті розробленої моделі до навченої нейромережі передається відбиток пальця із спеціального застосунку розробленої для android. Це

зображення передається в dateset та оброблюється за алгоритомом, який описаний вище. Після, за допомогою нейронної мережі відбувається пошук у базовому датасеті схожих за високорівневими ознаками зображень. Цей код використовує класифікатор (net), проте може вимагати змін у випадку, якщо ваша конкретна задача вимагає використання інших параметрів чи моделей.

Основні кроки включають зчитування та підготовку датасету, ініціалізацію для пошуку схожих зображень та паралельну обробку зображень за допомогою паралельного циклу (parfor). Кожне зображення змінює розмір та перетворюється для використання у класифікаторі, а відстань між вхідним та поточним зображеннями обчислюється та зберігається. Після завершення паралельного циклу результати конвертуються у масив, сортуються за відстанню, та виводяться перші 5 схожих зображень (рис. 4.5) та базове зображення у графічному інтерфейсі MatLab.

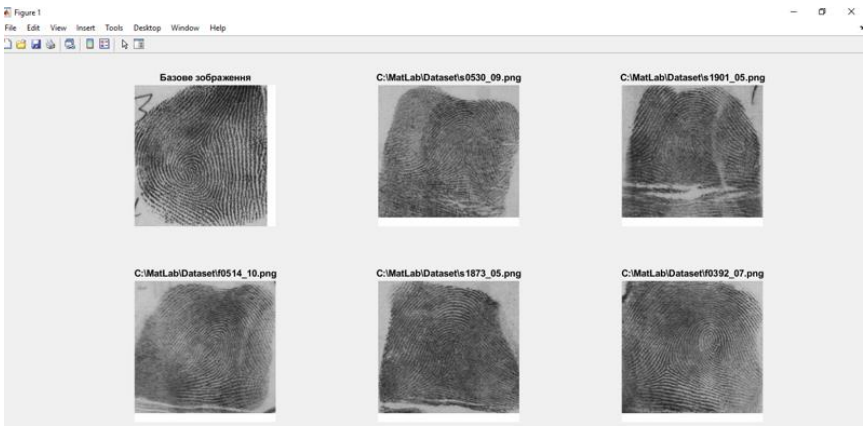

Рисунок 4.5 – Вивід візуалізації найбільш схожих зображень

Після повторної перевірки, з 5 зображень залишається 2 – надане в датасет, та те, що вже було у базі даних. Таким чином – доступ дозволено, або відмовлено, якщо ні одне із зображень не було знайдено.

ВИСНОВКИ

У даній кваліфікаційній роботі досліджено методи ідентифікації відбитків пальця за допомогою нейронної мережі та можливостей машинного навчання.

Було розглянуто основні поняття та методи ідентифікації відбитків.

Дослідження показало, що використання нейронних мереж для розпізнавання відбитків пальця є дієвим методом для забезпечення безпеки та контролю доступу до фізичних об'єктів. Точність і швидкість розпізнавання відбитків пальця залежать від якості навчання нейронної мережі і обсягу навчальних даних. Важливим аспектом є збір і зберігання великої кількості відбитків пальця для навчання мережі та враховування вимоги до безпеки та конфіденційності даних користувачів.

Практична цінність: способи використання згорткових нейронних мереж дозволяють досягти високої точності та стійкості у роботі системи навіть при великій різниці в особливостях відбитків зображень; переваги використання згорткової нейронної мережі та Resnet-50 є здатність до навчання на обмеженому обсязі навчальних даних, це важливо коли збір великої кількості даних може бути витратним або складним.

Наукова новизна в даному досліджені полягає у використанні сіамської нейронної мережі, як складової для подальшої ефективної обробки і аналізу великих обсягів даних відбитків пальців, здатність виявляти складні патерни незалежно від виду вхідного зображення.

Впровадження аналогічних систем може значно підвищити рівень безпеки та зручності в системах контролю доступу до фізичних об'єктів, де необхідний надійний контроль доступу, охорони об'єкту, що підвищує рівень безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Рагавендра, Р.; Буш, К.; Янг, Б. Надійна масштабована 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.

2. Yadava J. Development of Surface Acoustic Wave Electronic Nose. Defence Science Journal, 2010, 364-376.

3. Класичні методи шифрування інформації простою заміною Науковий вісник НЛТУ України. – 2011. – Вип. 21.9 – Львівський ДУ БЖД.

4. Потокова модифікація алгоритму rsa для шифрування зображень з чітко виділеними контурами / Ю. Рашкевич та ін. м. Львів. С. 171–178.

5. А. В. Жилін О. М. Шаповал О. А. Успенський. Технології захисту інформації в інформаційно-телекомунікаційних системах. Київ, 2020. С. 78–79.

6. Tilkov, S., & Vinoski, S. (2010). Node. js: Using JavaScript to build highperformance network programs. IEEE Internet Computing, 14(6), 80-83. – Режим доступу: https://ieeexplore.ieee.org/document/5617064

7. Luo P, Yu-Lun L.A., Wang Z. Hardware Implementation of Secure Shamir's Secret Sharing Scheme // High-Assurance Systems Engineering (HASE). IEEE 15th International Symposium. 9–11 Jan., 2014. DOI: https://doi.org/10.1109/ HASE.2014.34.

8. SSCC 2016 / SESSION 11 / SENSORS AND DISPLAYS / 11.2 3D Ultrasonic Fingerprint Sensor-on-a-Chip.

9. Banoula, M. An Overview on Multilayer Perceptron (MLP). Simplilearn. https://www.simplilearn.com/tutorials/deep-learning-tutorial/multilayer-perceptron.

10. Olah, C. Understanding LSTM Networks. Christopher Olah's Blog. https://colah.github.io/posts/2015-08-Understanding-LSTMs/. Опубліковано: 27 серпня 2015 року.

11. Каллан Р. Основные концепции нейронных сетей = The Essence of Neural Networks First Edition. — 1–ше. — «Вильямс», 2001. — С. 288.— ISBN 5–8459–0210–X.

12. Dong, C., Loy, C. C., He, K., & Tang, X. (2014, September). Learning a deep convolutional network for image super-resolution. In European conference on computer vision (pp. 184-199). Springer, Cham.

13. Парзіале, Г.; 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.

14. Захожай, О. І. (2013). Інформаційна технологія розпізнавання образів в задачах автоматизованої обробки інформації управління складними системами. Проблеми інформаційних технологій, (1), 61-68.

15. Виявлення закономірностей у параметрах методу Атебгабора для фільтрації біометричного зображення/ Режим доступу: https://journals.uran.ua/eejet/article/view/154862.

16. Мальтоні, Д.; Майо, Д.; Джайн, Аляска; Прабхакар, С. Генерація синтетичних відбитків пальців. У Довіднику з розпізнавання відбитків пальців ; Springer: Лондон, Великобританія, 2009; С. 271–302.

17. Dettmers T. How to Parallelize Deep Learning on GPUs Part 1/2: Data Parallelism [Електронний ресурс] / Tim Dettmers – Режим доступу до ресурсу:http://timdettmers.com/2014/10/09/deep-learning-data-parallelism/.

18. Ву, М.; Чен Л. Розпізнавання зображень на основі глибокого навчання. У матеріалах Китайського конгресу з автоматизації IEEE 2015 (CAC), Ухань, Китай, 27–29 листопада 2015 р.

19. Life cycle models, principles and methodologies of software development / Rozhnova Tatyana, Tomachynska Valeriia, Korsun Denis // Proceedings of the 7th

International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (December 19-20, 2022). Rome, Italy. INFORMATION AND WEB TECHNOLOGIES №137 DOI 10.51582/interconf.19-20.12.2022.040

19. Корсун Д. М., Рожнова Т. Г. Система криптографічного захисту bluetooth зв'язку симетричним алгоритмом блокового шифрування. Комп'ютерної інженерії та захисту інформації : МАТЕРІАЛИ 27-го МІЖНАР. МОЛОДІЖ. ФОРУМУ, м. Харків, 10 трав. 2023 р. Харків, 2023. С. 59–60.

20. Корсун, Д.М. Методи розпізнавання відбитків пальців за допомогою нейронних мереж. Тези III Міжнародної студентської наукової конференції «Міждисциплінарні наукові дослідження та перспективи їх розвитку». 10 листопада 2023 р., м. Дніпро. С. 120–123.

21. Tomachynska V. S., Korsun D. M., Rozhnova T. H. Life cycle models, principles and methodologies of software development. Theory and practice of science: key aspects : Proceedings of the 7th International Scientific and Practical Conference, Rome, 20 December 2022. 2022. P. 394–401.