Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод створення гібридної системи ідентифікації особи за біометричними даними

(тема)

Виконав:

студент II курсу, групи СПм-22-1

Тарасянц А.А.
(прізвище, ініціали)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва освітньої програми)

Керівник: проф. Міхаль О.П.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Тарасянц Аліні Арсенівні
(прізвище, ім'я, по батькові)

1. Тема роботи Метод створення гібридної системи ідентифікації особи за біометричними даними

затверджена наказом по університету від " 06 " листопада 2023 р. № 1299Ст

2. Термін подання студентом роботи до екзаменаційної комісії 12 січня 2024 р.

3. Вхідні дані до роботи
Arduino
Методи біометрії
Пристрої зчитування біометричних характеристик

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз проблем та існуючих рішень ідентифікації
Аналіз видів ідентифікації
Технології ідентифікації осіб за біометричними характеристиками
Розробка методу гібридизації
Експеримент та тестування рішення
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 16 слайдів

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз завдання	07.11.2023-09.11.2023	
2	Аналіз науково-технічної літератури	10.11.2023-11.11.2023	
3	Пошук існуючих рішень	12.11.2023-15.11.2023	
4	Розробка і тестування методу гібридизації	16.11.2023-20.11.2023	
5	Оформлення пояснвальної записки	21.11.2023-28.11.2023	
6	Оформлення графічної частини	29.11.2023-03.12.2023	

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Міхаль О.П.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 84 с., 31 рис., 2 табл., 1 дод., 15 джерел.

ІДЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ ХАРАКТЕРИСТИКИ, ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ, ГІБРИДИЗАЦІЯ.

Метою кваліфікаційної роботи є розробка метода створення гібридної системи ідентифікації особистості. Розроблена система буде мати більш гнучку, швидку та надійну роботу з подальшими впровадженням задля поліпшення та зручного використання.

У ході виконання кваліфікаційної роботи прводений аналіз існуючих рішень ідентифікації особи за біометричними даними. Розглянуто переваг, недоліків, технологій використання і відповідно розробка метода створення гібридної системи ідентифікації особистості.

ABSTRACT

Master’s thesis: 84 pages, 31 figures, 1 tables, 2 appendices, 15 sources.

IDENTIFICATION, BIOMETRIC CHARACTERISTICS, IDENTIFICATION TECHNOLOGIES, HYBRIDIZATION.

The major goal of this thesis is to develop a method for creating a hybrid system of personal identification. The developed system will have a more flexible, fast and reliable operation with further implementations for improvement and convenient use.

In the course of the qualification work, an analysis of existing solutions for identification of a person based on biometric data was conducted. The advantages, disadvantages, technologies of use and, accordingly, the development of a method for creating a hybrid system of personal identification are considered.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

RFID – радіочастотна ідентифікація (англ. Radio Frequency IDentification).

ДНК – дезоксирибонуклеїнова кислота.

ISO – міжнародна організація щодо ратифікації стандартів (англ. International Organization for Standardization).

ЕКГ – електрокардіографія.

OLED – органічний світлодіод (англ. Organic Light-Emitting Diode).

SoC – система на чипі (англ. System-on-a-Chip).

ASR – автоматичне розпізнавання мовлення (англ. Automatic Speech Recognition).

ML – машинне навчання (англ. Machine Learning).

RR – відстань між двома точками в ЕКГ.

DAQ – система збору даних (англ. Data Acquisition).

ВСТУП

Інформаційне суспільство активно розвивається, відповідно інформаційно-комунікаційні технології також змінюються. В технологічному сучасному світі безпека даних та інформації стоїть на першому місці для людства. Забезпечення надійного захисту інформації включає в себе різні аспекти та засоби, спрямовані на збереження цілісності та конфіденційності даних. Захист інформації є надзвичайно важливим викликом для організацій у сучасному цифровому світі, оскільки щодня загроза хакерів зростає.

Сучасні методи ідентифікації особи не можуть забезпечити необхідний рівень надійності та захисту. Порушення конфіденційності або доступності до даних прийнято недооцінювати і сподіватися на краще, що нікому не потрібна жодна інформація. Але, як показує статистика, щодня рівень підробки, порушення і викрадення особистих даних лише зростає. Тому, рішенням є створення гібридної системи ідентифікації осіб за біометричними даними.

Ідентифікація особи – процес встановлення особи, підтвердження її особистих даних. Для цього існує багато різних методів і процесів, які можна використовувати: розпізнавання обличчя, відбитки пальців, паролі, пін–коди, магнітні картки тощо. Біометричні технології використовуються в багатьох областях, де потрібен захист інформації.

Повсякчас ідентифікація особи буде актуальна, у зв’язку з тим, що світ розвивається і технології кожного дня змінюються та покращуються. Більшість послуг стають цифровими, тому ідентифікація особи має значення в багатьох сферах життя і допомагає забезпечити захист важливих даних, інформації тощо.

Завдання кваліфікаційній роботі полягає в тому, щоб створити гібридну систему ідентифікації особистості за біометричними даними для вдосконалення захисту та швидкості роботи.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

1.1 Сучасні методи ідентифікації за біометрією

З появою онлайн-роботи, дистанційного навчання, доступності цифрових документів тощо конфіденційна інформація з кожним днем стає все більш поширеною і менш захищеною. Тому актуальним на сьогодні є питання ідентифікації особистості, а також захисту цих даних [9].

Наразі існує декілька варіантів ідентифікації людини:

- парольна ідентифікація;
- біометрична ідентифікація;
- апаратна ідентифікація.

Кожен зі способів ідентифікації має свої переваги й недоліки.

Парольна ідентифікація – одна з перших систем, яка з’явилася для визначення особистості. Проста у використанні, не потребує складних програм або засобів, що є перевагою. Проте надійність і безпека такого типу ідентифікації є великим недоліком. Вважається, що отримати доступ до особистих даних простіше саме через парольну ідентифікацію.

Апаратна ідентифікація – процес, який заснований на визначені особистості за якимось предметом, електронним ключем тощо. Обидва види ключів, що використовуються при апаратній ідентифікації мають переваги і недоліки.

Карткові ключі – ненадійний засіб ідентифікації, який легко можна пошкодити механічно. З переваг є лише простота реалізації і використання.

Надійним засобом апаратної ідентифікації є пристрої з власною пам'яттю - токени. Тому що при їх використанні можна використовувати двофакторну ідентифікацію особи. Двофакторна ідентифікація означає, що спочатку користувач надає ключ (наприклад, генерує відкритий ключ), а потім система чекає дії від особи для його підтвердження (наприклад,

введення пароля або пін-коду, який був визначений заздалегідь).

До того ж існує штрих-код для апаратної ідентифікації особистості. Найчастіше такий тип ідентифікації використовують в торгівлі товаром різноманітних сфер. Однак для користувачів така система також можлива у використанні, лише надається унікальний штрих-код, яким особа можна скористатися. Значним недоліком штрих-кодів є те, що їх легко підробити.

Радіочастотна ідентифікація (RFID) потребує наявність двох пристроїв – пристрій зчитування і RFID-позначки. Інформація для ідентифікації особистості зберігається у позначці, яка при необхідності ідентифікації надається пристрою зчитування. Обмін даними виконується за допомогою радіосигналів. Перевагою є відсутність прямого контакту з особою. Недоліками є вартість пристроїв, викрадення або втрата RFID-позначки, а також можливість переривання сигналу.

В області інформаційних і цифрових технологій біометрична ідентифікація – це одна з найновіших методів ідентифікації осіб. Біометричні дані – унікальні фізичні / морфологічні / поведінкові риси людини, завдяки яким можна ідентифікувати або перевірити особу. Кожна особа має унікальність, тому малоймовірно їх підробити, відповідно до цього біометричні дані досить швидко набрали актуальність для забезпечення безпеки ідентифікації.

Складність впровадження біометричної системи ідентифікації за допомогою біометричних ознак можна пояснити двома недоліками. Менш важливою є можливість фальсифікації деяких біометричних даних.

Біометрична ідентифікація містить взаємопов’язані напрями – статичні та динамічні [1]. До статичних (фізіологічних) відносяться фізіологічні ознаки, за допомогою яких можна ідентифікувати людину. Це ті унікальні ознаки, які характеризують людину від народження і ніяк не залежать від психічного стану людини. Динамічні ознаки (психологічні) – ознаки, основані на поведінці особистості під час будь-якої дії. Вони легше у реалізації та використанні, не вимагають додаткових приладів, програмних

забезпечень.

До фізіологічних ознак відносяться:

- відбитки пальців;
- ДНК (дезоксирибонуклеїнова кислота – це біомолекула, яка містить генетичну інформацію);
- геометрія вуха;
- райдужна оболонка ока;
- розташування вен на долонях;
- геометрія обличчя;
- сітчатка ока.

Психологічні ознаки є менш надійними, так як поведінка у певних ситуаціях і людях є не постійно однаковою. До психологічних ознак відносяться:

- голос;
- серцебиття;
- почерк.

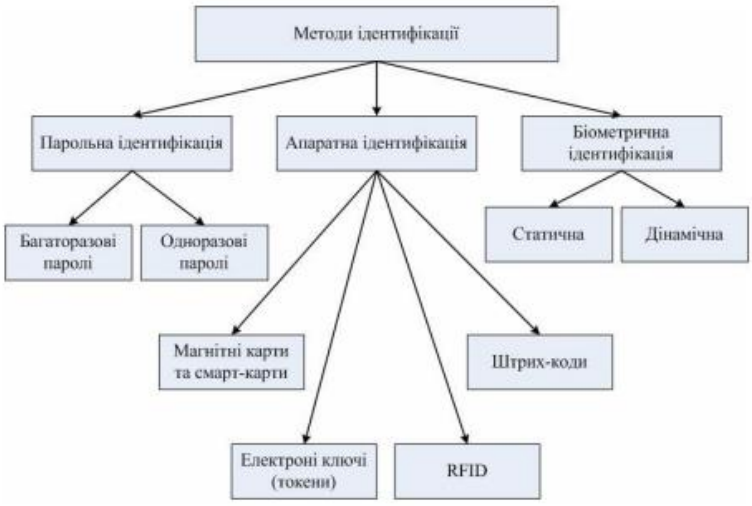

Рисунок 1.1 – Класифікація методів ідентифікації

Перелічені вище методи ідентифікації людини є найактуальнішими і

дозволяють ідентифікувати людину майже повністю. Крім того, досі людство і технології продовжують знаходити і створювати нові методи ідентифікації.

Наразі існує єдина система форматів обміну біометричними даними – стандарт формату даних біометричних ідентифікаторів (Biometric Data Interchange Formats), який регламентується міжнародними організаціями (ICAO та ISO). Стандарт визначає формати обміну біометричними даними (відбитками пальців і т.д.), які використовуються для ідентифікації особистості в різних сферах. Ця система допомагає забезпечити єдиний обмін біометричними даними між організаціями, органами влади та навіть країнами для безпеки та надійності особистих даних [6].

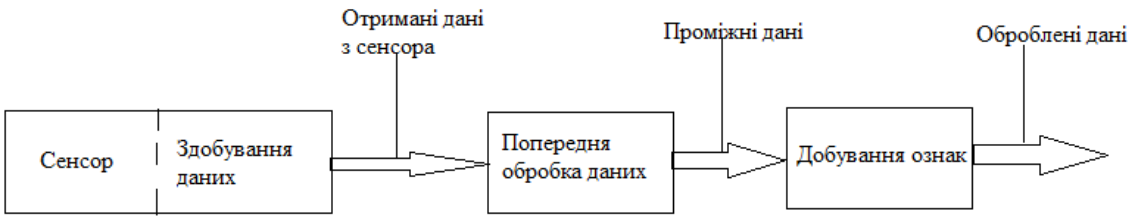

Рисунок 1.2 – Схема процеса обробки біометричних даних

Етапи ідентифікації особистості та, відповідно, створення гібридної системи за біометричними даними складається наступним чином:

- збір біометричних даних. Як зазначено вище, є багато біометричних методів для визначення особи завдяки камерам, сенсорам тощо;
- обробка зібраних даних для визначення особи, яка є на етапі ідентифікації;
- збереження отриманої інформації з шифруванням у безпечних базах даних або на хмарах з шифруванням для надійногості;
- створення біометричного шаблону для подальшого порівняння;
- безпосереднього порівняння отриманих даних про особу та вже наявних;
- прийняття рішення після порівняння даних;

- відповідь системи про відповідність особистості та наявних даних або навпаки – невідповідність даних і особи.

Процес обробки біометричних даних – це складна процедура, яка містить збір, зберігання, обробку та використання біометричних даних для подальшої ідентифікації особистості. В цей процес можуть бути долучені спеціалізовані програми та обладнання, які більш точно і якісно обробляють отримані дані, зберігають їх для подальшого використання [11].

Типове обладнання для обробки біометрії: сканери (для відбитків пальців), камери (для фіксації та розпізнавання обличчя).

Використовується програмне забезпечення, яке може обробляти дані з обладнання. Наприклад, існує OpenCV (Open Computer Vision Library) – бібліотека комп'ютерного зору, можна використовувати для обробки зображень обличчя осіб. MySQL – реляційна система управління базами даних, де можна зберігати біометричні дані.

В процесі обробки біометричних даних важливо надати надійний захист, щоб уникнути несанкціонованого доступу до даних. Наприклад, додаткове шифрування даних різними методами, додаткова аутентифікації до систем зберігання біометричних даних.

Для валідації отриманих даних і їх подальшого використання потрібні алгоритми, які можуть бути реалізовані в програмному забезпеченні. Для ефективної обробки отриманих даних потрібні високопродуктивні обчислювальні сервери.

1.2 Основні види біометричних даних для визначення особистості

Біометричні дані використовуються для ідентифікації особистості на основі фізіологічних чи поведінкових характеристик [10]. Основні види біометричних даних включають:

- відбитки пальців;
- розпізнавання обличчя;

- розпізнавання райдужної оболонки ока (ірису);
- голосовий аналіз;
- аналіз системи вен долоні або руки;
- аналіз письма;
- електрокардіограма (ЕКГ);
- ходьба людини.

Відбитки пальців – один з найпопулярніших засобів для визначення особистості. Кожна людина має унікальні точки та лінії на пальцях, завдяки яким можна її ідентифікувати. На рисунку 1.3 зображено палець із детальною будовою унікальних папілярних ліній, кінцевих точок, які є унікальними.

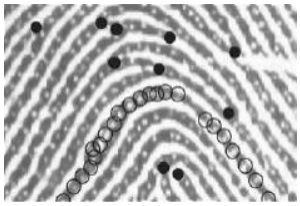

Рисунок 1.3 – Відбиток пальця з відміченими порами, кінцевими точками

Збір біометричних даних передбачає сканування поверхні певного пальця або всіх для отримання детального зображення папілярних ліній, точок та інших характеристик. Дані з відбитків пальців можуть зберігати в цифровому вигляді, для чого не обов’язково використовувати додатковий захист.

Відбитки пальців використовуються для розблокування різних пристроїв (телефон, планшет, ноутбук тощо), для ідентифікації особи перед наданням доступу до захищених даних, для контролю доступу (наприклад, при вході в офіс), для ідентифікації особи у вищих органах охорони, для підтвердження фінансових транзакцій, для митного контролю і т.д.

Овал обличчя, розташування очей, носа, рота, брів тощо вважаються фізичними характеристиками для ідентифікації особистості.

Перш за все, камерами фіксують обличчя з різних сторін і при різному

освітленні для якісного фіксування всіх особливостей обличчя людини. Отримане зображення обробляється і важливі та унікальні точки зберігаються (розташування брів, очей, рота тощо). Далі створюється шаблон, по якому надалі роблять порівняння і приймається рішення, чи відповідає особа тій, яка раніше ідентифікувалася.

Найчастіше розпізнавання обличчя забезпечує безпеку при вході до приміщень, розблокування пристроїв і навіть у медичних діагностиках.

Ірис – кольорова частина ока, яка знаходиться між рогівкою та склерою, є унікальною для кожної людини. Тому технологія розпізнавання райдужної оболонки ока – один з надійних методів через те, що очі людини та їх особливості важко підробити.

Зазвичай ірис фотографують камерою, яка здатна спрямовувати свій фокус на деталі для аналізу рисунку, включаючи розташування пігментів, вен тощо. На основі отриманих даних створюється шаблон, по якому потім ідентифікують людину.

Перевагою даного виду біометричних даних полягає в тому, що ірис настільки індивідуальний, що надає високу точність і надійність ідентифікації особи навіть при поганому освітленні. Використовується даний метод найчастіше в системах безпеки, аутентифікації на робочому місця тощо.

Голосова біометрія – аналіз голосу людини для ідентифікації особистості. Людський голос, як і відбиток пальця або ірис, унікальний.

Цей метод ґрунтується на тому, що кожна людина має унікальні особливості голосу, такі як тембр, інтонація, швидкість та інші характеристики. Для голосового аналізу використовуються спеціальні технології, які записують та аналізують зразки голосу.

Кожна особистість має унікальні вени та також є одним з декількох надійних методів для перевірки особи. Вид біометричних даних, який заснований на зчитуванні малюнків вен на долонях особи, аналізі та збереженні.

Венна структура долоні не змінюються протягом усього життя, тому цей спосіб вважається одним з найнадійніших варіантів. Інформація про систему вен не доступна всім користувачам, тому їх майже неможливо підробити.

Перевагою є те, що для зчитування системи вен долоні використовуються інфрачервоні камери. Це дозволяє здійснювати ідентифікацію без контакту, що важливо у гігієнічних заходах. Доволі часто такий вид ідентифікації використовуються в медичних закладах або банках.

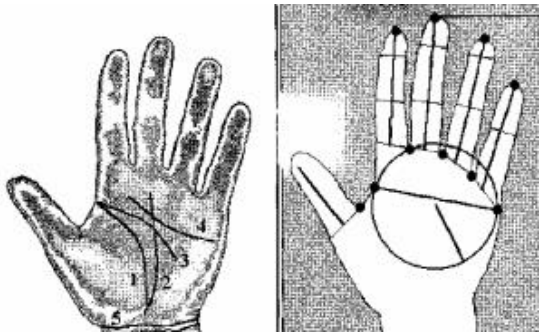

Рисунок 1.4 – Аналіз долоні

Недоліком аналізу системи вен долоні є вимоги до обладнання, що може бути досить коштовним, складнощі в обслуговуванні, захист зібраних даних, вплив зовнішніх факторів (поранення, захворювання і т.д.).

Графологія (аналіз письма) – це вид біометричних даних, з якими можна аналізувати людину по таких критеріях: швидкість, тиск, напрямок письма, інтервали між буквами та словами, графічні елементи, спосіб і навіть якою саме рукою пише особа (лівою / правою). Вона не є науково обґрунтованою і надійною, проте використовується в багатьох сферах.

Тому вважається, що ідентифікація особи на основі біометричних даних, таких як відбитки пальців, розпізнавання обличчя, аналіз ірису та інші, є більш надійними та обґрунтованими методами, які використовуються в сучасних системах безпеки.

Біометрія ходьби є способом ідентифікації людини на основі її

унікального способу ходьби. Зокрема: рух ніг, схилення, кут вибиття, постійність кроків у хвилину, відбиток унікальний як відбиток пальців. Перевагою можна вказати, що по ходьбі ідентифікувати особистість можна на відстані [2].

Системи біометрії ходьби використовують різні технології для збору та аналізу даних про ходьбу, такі як камери, акселерометри, гіроскопи та інші сенсори. Ці дані потім можуть бути використані для створення унікального біометричного шаблону особи. Використання є в різних сферах, включаючи безпеку, військову та цивільну ідентифікацію та контроль доступу.

Електрокардіограма (ЕКГ) – це графічне зображення електричної активності серця, яке відображається у вигляді кривої на папері або на екрані монітора. Ця крива відображає зміни в електричному потенціалі серця в часі й використовується для діагностики різних серцевих захворювань та вимірювання пульсу.

ЕКГ може бути використаною як біометричний параметр в системах ідентифікації осіб, таких як біометричні сканери або системи розпізнавання осіб на основі фізіологічних ознак. Принцип роботи полягає в тому, що певні характеристики ЕКГ можуть бути унікальними для кожної людини, а отже, їх можна використовувати для ідентифікації.

Головною перевагою є висока стабільність серцевих симптомів у часі та складність імітації. Однак біометричні системи мають технічні та практичні проблеми, такі як забезпечення безпеки та конфіденційності даних, а також розробка спеціальних датчиків і алгоритмів обробки сигналів.

Основною метою ідентифікації особи за біометричними даними – переконання, що людина є тією, за кого себе видає. Це може бути корисним в різних контекстах, таких як безпека, доступ до приватної інформації, контроль доступу, аутентифікація та інші сфери. Використання біометричних даних може зробити процес ідентифікації більш зручним для користувачів, оскільки вони не повинні запам'ятовувати паролі або носити з собою ключі чи картки. А також системи можуть вести журнал ідентифікаційних

операцій, що дозволяє відстежувати, коли й де була виконана ідентифікація.

Можна зробити висновки, що існує безліч варіацій ідентифікації особистості різного формату, де потрібне спеціальне обладнання та ні, де потрібна фізична присутність людини та ні, де потрібні додаткові картки та ні. Тому масштабною єдиною різницею є надійність і захист даних для ідентифікації від хакерів.

1.3 Гібридизація методів ідентифікації особи

Вищеперелічені види біометричних даних можна використовувати окремо для визначення особи або вибрати декілька для створення гібридних систем ідентифікації особи. Коли використовується декілька засобів біометричних даних, то процес визначення особистості є більш безпечним та надійним [13].

Рисунок 1.5 – Пристрій зчитування декількох біометрих даних (відбитки пальців і вени на долоні)

Гібридизація методів – це підхід, який поєднує комбінацію кількох методів (в нашому випадку декілька видів біометричних даних), для досягнення найточнішої ідентифікації особи. Гібридизація методів може бути

корисною там, де одна технологія має обмеження або недоліки, і поєднання її з іншими може призвести до більш ефективних та вдалих рішень.

Гібридна система ідентифікації особи з використанням біометричних даних передбачає комбінування двох або більше видів біометрії. Перш за все, перевагою гібридизації є захист від атак, надійність і безпека збереження даних. Це пов’язано з використанням декількох видів захисту і перевірки. Таким чином складніше отримати непрямий доступ до біометричних даних.

Наприклад, система може просканувати відбиток пальця особи та вени на долоні, а потім – потрібно ввести пін-код. Таким чином, навіть якщо пін–код буде викрадений, то біометричний вид ідентифікації підробити набагато складніше.

Наступна перевага – точність ідентифікації. Створені бази даних зберігають усі зібрані біометричні дані особи, часто кількох типів одночасно. Це дозволяє точно ідентифікувати особу, оскільки система автоматично шукає всю інформацію для перевірки.

Наприклад, спочатку можна взяти відбиток пальця, по якому на сервері шукають всі збіги. Далі – спеціальним приладом просканувати оболонку ока людини та по базі даних знайти збіги. Таким чином, відповідність особи буде точною.

Також перевагою є зручність для користувачів. У разі ідентифікації особи, наприклад, на веб-сайті, у користувача буде можливість вибрати зручний спосіб. Наприклад, при швидкій авторизації можна ввести пін–код або використати біометричні дані, які заздалегідь користувач додав на свій акаунт.

Гібридні системи та методи ідентифікації можна швидко адаптувати до новітніх технологій або в залежності від сфери використання.

Однак слід мати на увазі, що гібридні системи ідентифікації інколи складно реалізувати. Оскільки пристрої досить дорогі, програмне забезпечення та сервери потребують технічної підтримки завжди. Оскільки гібридні системи зберігають багато конфіденційної інформації, важливо

забезпечити належний рівень безпеки та конфіденційності.

Незважаючи на те, що гібридизація методів є ефективною та надійною, вона має і недоліки. Отже, складність реалізації та використання є недоліком такого методу ідентифікації особистості. Іноді система потребує правильної комбінації приладів, програмного забезпечення і технічної підтримки у майбутньому використанні.

З цього виникає другий недолік – залежність від коректної роботи повного набору обладнання і програмних додатків. Таким чином, гібридна система завжди потребує постійної підтримки, оновлення і модернізації систем в залежності від розвитку інформаційних технологій.

Чим більше варіантів отримує система при ідентифікації людини, тим вище ймовірність помилкової ідентифікації. Помилкове визначення людини ймовірно, оскільки в будь-якій системі можливий випадок невірної ідентифікації через великий обсяг даних.

Впровадження гібридної системи ідентифікації може бути дорогим. Створення системи вимагає великих капітальних вкладень для придбання, подальшої підтримки та обслуговування необхідного обладнання.

З моменту формування цифрових та інформаційних технологій загроза порушення безпеки даних зростає. Завжди існує небезпека у вигляді різноманітних атак, вторгнень, які порушують або зчитують біометричні дані, існує весь час. Тому не варто нехтувати безпекою і захистом даних.

Часто в системах ідентифікації особи увага приділяється саме на біометричні методи ідентифікації. Найбільш ефективний захист забезпечують гібридні системи, в яких біометричні засоби комбінуються з апаратними пристроями ідентифікації. Або в якості альтернативи можна використовувати технічні можливості розпізнавання особистості, які складаються з речового ідентифікатора (ключа), інформаційно-смислового ідентифікатора (зазвичай пін-код або пароль, що вводиться людиною) і біометричного ідентифікатора.

Комбінуючи декілька засобів, можна створити більш захищену систему

визначення ідентифікації особи. І таким чином система виходить на більш оптимальний рівень вартості та ефективності визначення особистості.

Підсумовуючи, гібридизація методів ідентифікації особи за біометричними даними набуває багато переваг і згодом охоплює багато сфер для використання. Через те, що гібридність дає змогу поєднувати в собі безліч видів ідентифікації, в залежності від запитів і сфери використання.

1.4 Постановка задачі

Задачею кваліфікаційної роботи є аналіз існуючих рішень ідентифікації особи за біометричними даними. Розгляд переваг, недоліків, технологій використання і відповідно розробка метода створення гібридної системи ідентифікації особистості. Розроблена система буде мати більш гнучку, швидку та надійну роботу з подальшими впровадженням задля поліпшення та зручного використання.

2 ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА БІОМЕТРИЧНИМИ ХАРАКТЕРИСТИКАМИ

2.1 Технології відбитків пальців

Сучасні методи ідентифікації за допомогою біометричних даних вважаються досить захищеними, винятковими та індивідуальними [7]. Різноманітність методів дає змогу детально аналізувати технології та їх використання [12].

Розповсюджений засіб ідентифікації особистості є відбитки пальців, наприклад – Touch ID компанії Apple. Технологія Touch ID компанії Apple стала проривом в області аутентифікації за допомогою відбитка пальця, вважається одним із найдосконаліших апаратних і програмних засобів.

Введення пін-кода або паролю є ненадійним і вразливим до помилок. Оскільки досить складний пароль займає багато часу при введенні, тому користувачі були змушені вигадували менші за кількістю символів паролі, що призводило до викрадення даних з пристроїв.

Отже, з часом компанія Apple для вирішення питання безпечної ідентифікації особистості розробила технологію Touch ID. Touch ID – датчик ідентифікації за відбитками пальців.

В більш старих моделях пристроїв датчик розпізнавання пальців знаходився в кнопці «Додому», як зображено на рисунку 2.1.

Стійка до подряпин лінза із сапфірового скла сканувала відбиток пальця. Сталеве кільце оточує лінзу, аналізує наявність пальця та надає повідомлення датчику Touch ID для зчитування палеця. Коли система спрацювала – вмикається датчик і відбиток пальця сканується з високою роздільною здатністю. Потім він створює математичне представлення вашого відбитка пальця та порівнює його із зареєстрованими даними відбитка пальця, щоб визначити збіг і розблокувати пристрій.

Потім, щоб ідентифікувати власника пристрою, отриманий відбиток пальця порівнюється з Secure Enclave (захищені анклави — це пов’язані з безпекою набори кодів інструкцій, вбудовані в нові процесори) на чіпсеті Apple A7 (64-bit 2) мікропроцесора Apple ARM із серією Apple Axe).

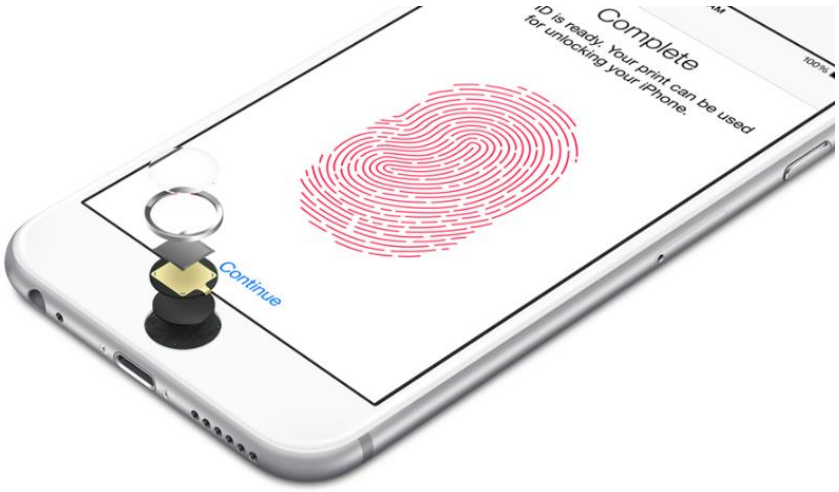

Рисунок 2.1 – Touch ID на пристрої компанії Apple

Дані відбитків пальців зашифровані, зберігаються на диску та захищені ключем, доступним лише для Secure Enclave. Якщо унікальність збігається по лініях, порах та кінцевих точках, то аутентифікація особистості успішна і пристрій розблоковано.

Перевагою даного методу ідентифікації особи є зручність і швидкість. Сенсор Touch ID має тонку пластину, яка може сканувати 550 пікселів на дюйм. Це забезпечує хороший рівень деталізації пальців.

Також перевагою є сканування пальців на підшкірному рівню, а не поверхнево. Вважається, що поверхневий рівень пальця постійно оновлюється, тому краще сканувати саме підшкірний рівень. Відповідно до цього у разі викрадення відбитків пальця у людини, враховуючи оновлення шкіри, менш вірогідно підробити та просканувати відбиток.

Наступним є те, що сканер може запам’ятати повний обсяг пальця і в цілому більше одного пальця. Це зручний спосіб для, наприклад, людей, які

при ходьбі тримають пристрій в одній позі та зручно один палець відсканувати. В робочий час, сидячи за столом, зручно проскановувати інший.

Але є кілька ситуацій, коли датчик блокується і не надає доступу, що є недоліками:

- якщо відбиток пальця не є унікальним більше 5 разів, пристрій буде заблоковано до введення пароля або пін-коду;
- після перезавантаження пристрою перше розблокування здійснюється лише паролем або пін-кодом;
- якщо датчик Touch ID не використовується протягом двох днів, необхідно ввести пароль або пін-код;
- для безпеки в разі викрадення пристрою існує дистанційне блокування.

Операційна система Android також використовує датчик відбитків пальців, який є менше за обсягом, проте зчитує великий обсяг пальців. Існує три технології зчитування відбитків: ємнісна, ультразвукова та оптична.

Оптичний зчитувач встановити можна на OLED-екрани (Organic Light Emitting Diode – світловипромінюючі органічні дисплеї) і є більш сприйнятливим до підробки. Являє собою камеру, яка може фотографувати палець.

За принципом своєї дії такі сканери схожі на цифровий фотоапарат. Прикладаючи до датчика палець, той підсвічується. Світло відбивається від поверхні пальця і потрапляє на світлочутливу матрицю, яка оптичний сигнал перетворює на цифровий. І таким чином стає видно рельєфний малюнок відбитка, який система аналізує.

Переваги оптичного датчика є можливість встановлення під екран пристроїв різного формата. Проте є значні недоліки:

- яскравість підсвітки сканера автоматично не регулюється;
- не завжди спрацьовує з захисним склом або плівкою;
- не спрацьовує при наявності забруднень на пальцях;

- роздільна здатність світлочутливої матриці впливає на швидкість роботи самого сканера.

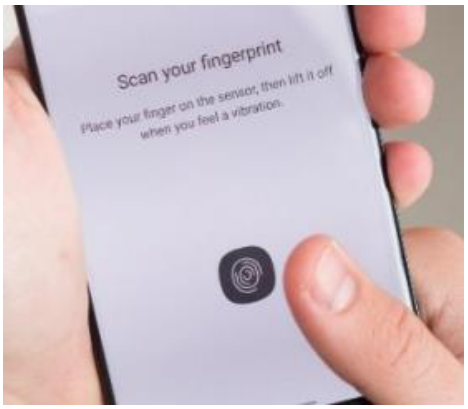

Рисунок 2.2 – Оптичний датчик зчитування відбитків пальців

Ємнісний датчик зчитування відбитків пальців складається з декількох маленьких конденсаторів, які накопичують електроенергію, що розряджається в місцях, де торкаються частини пальця. Такий вид не можна встановити під дисплей.

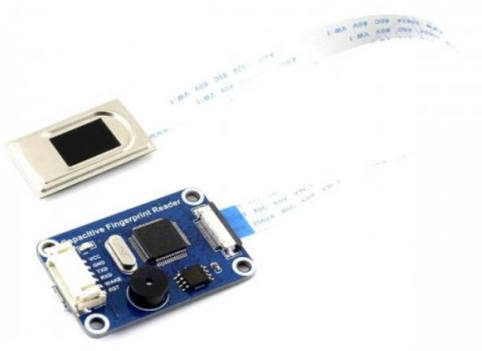

Рисунок 2.3 – Ємнісний датчик зчитування відбитків пальців

Чим більше роздільна здатність, тим більше струмопровідних частин, яких торкається палець при збору відбитків. Відповідно при дотику пальцем сканеру заряд, який знаходиться в конденсаторі, відтворює відбиток.

Переваги емнісного сканера:

- швидкість;
- низька вартість;
- працює у разі якщо палець брудний або вологий;
- надійність;
- стабільність;
- точність.

Недоліки:

- не встановлюється під екран (тобто можна використовувати лише на пристроях, де є кнопка).

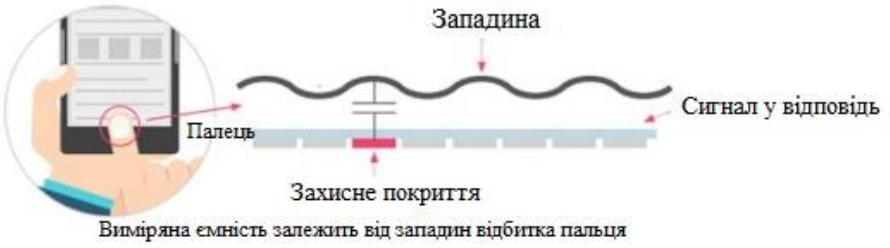

Рисунок 2.4 – Принцип роботи ємнісного датчика

Найкращий вид датчиків для сканування відбитків пальців вважаються ультразвукові. Це досить нова технологія, яку нещодавно почали використовувати лише американська компанія Qualcomm, яка виготовляє процесори Snapdragon (сімейство мобільних систем на кристалі (SoC)).

Принцип роботи ультразвукового зчитувача: електричний струм створює звуковий імпульс, який передається на ваш палець при доторканні до екрана. Він знову повертається до сканера та ультразвуковий сигнал перетворюється на цифровий для подальшої роботи процесора.

Перевагами даного типу є безпека, бо сканування відбитка пальця йде 3Д. Наступним виключенням є встановлення сканера у будь-якій частині пристрою. Ультразвук дозволяє зробити захист більш надійним через те, що ніби сигнал проникає в палець.

Головною різницею трьох видів датчиків є отримання відбитків пальців. Оптичний отримує за допомогою світла. Ємнісний – за допомогою струму. І відповідно ультразвуковий – завдяки звуку. Технологія розпізнавання відбитків пальців стала важливою функцією телефонів Android. Вона пропонує швидкий і зручний спосіб розблокування пристрою, гарантуючи безпеку.

Як правило, біометрія відбитків пальців використовується в різних сферах життя. Такий вид ідентифікації широко використовується для виявлення підозрюваних і злочинців. У військовій сфері зі відбитками можна визначити ворогів і союзників. Охорона здоров’я використовує даний вид біометрії для зберігання особистих даних.

Використання відбитків пальців в смартфонах є так званим стандартом в сучасному житті. Значний недолік – захисні плівки або скло на пристрої може притворможувати роботу сканеру. Порізи, рани можуть стати також перешкодою для отримання відбитка пальця. Сенсори досить чутливі та гарно розпізнають відбитки, коли пальці чисті. Але для будівництва чи виробництва, наприклад, даний вид ідентифікації не завжди може працювати.

Наступним недоліком є вартість системи контролю, збору та зберігання відбитків пальця. Для масштабних компаній або де працівники працюють в різних куточках світу відбитки пальців для ідентифікації можуть коштувати великих коштів.

Значеним упущенням іноді стає викрадення відбитків пальців або підробка. Найчастіше дані зберігаються у локальних базах даних, що є не досить безпечним.

Точність не висока у порівнянні з іншими видами біометричних характеристик для ідентифікації. Універсальність та швидкість розпізнавання даного методу є досить проблемними. Враховуючи, що системи контролю сильно залежать від апаратного забезпечення, то можуть виникати проблеми з продуктивністю.

Біометричні зчитувальні пристрої схильні до двох видів помилок:

- частота хибних прийомів (FAR);
- частота хибних відхилень (FRR).

Коли система приймає неавторизовану особистість – FAR, коли система відхиляє авторизовану особистість – FRR. Був проведений експеримент для великих виробництв і отримали поганий результат, що помилки виникають приблизно 1%, то для 1000 осіб 100 отримують відмову в ідентифікації, що є досить значним.

2.2 Технологія розпізнавання обличчя

Інноваційні засоби розвиваються щодня, тому можна побачити, що виробники активно відмовляються від використання відбитків пальців у ідентифікації особистості та переходять до новітнього способу – розпізнавання обличчя.

Face ID – це інноваційний метод аутентифікації за допомогою розпізнавання обличчя. Face ID – інтуїтивно зрозумілий і надійний метод аутентифікації, який заснований на структурному відображенні обличчя за допомогою передових технологій і системи камер TrueDepth (складна система датчиків і камер).

Камера отримує дані обличчя особистості, шляхом проектування на ньому безліч точок. Пристрій для зчитування аналізує і відтворює ніби карту обличчя, а також зображення в інфрачервоному спектрі. Фрагмент Neural Engine процесорів, який захищено модулем Secure Enclave, перетворює структурну карту й інфрачервоне зображення на математичну модель, яка порівнюється із зареєстрованими даними обличчя.

Перевагою є те, що датчик Face ID автоматично адаптується до невеликих змін зовнішнього вигляду людини. У разі важливих змін (наприклад, новий колір волосся або вигляд бороди) система запропонує ввести пароль або пін-код для підтвердження вашої особи.

Також перевагою є те, що камера TrueDepth автоматично активується, коли піднімається пристрій або відбувається торкання екрана, щоб вивести його з режиму сну, а також коли надходить сповіщення, яке вмикає екран. Щоразу, як розблоковується пристрій, камера TrueDepth розпізнає обличчя, при цьому зчитує точні структурні дані й інфрачервоне зображення.

Зареєстровані дані Face ID для безпеки шифруються ключем, який доступний лише для модуля Secure Enclave. Ймовірність, що розпізнаванням стороннім обличчям відбудеться, дорівнює майже нулю. Face ID порівнює дані про структуру обличчя, які неможливо отримати з друкованої або цифрової фотографії. А передові нейронні мережі захищають від шахрайства за допомогою масок та інших прийомів.

Проте, наразі є не вдосконалення в даній системі, а саме – сканер може спрацювати та надати доступ до пристрою, якщо датчик проскакує схожого брата / сестру. Тому, в плані безпеки вважається кращим Touch ID.

Face Unlock – це технологія, розроблена компанією Google і використовується користувачами для розблокування пристроїв за допомогою сканування обличчя. Розпізнавання обличчя складається з трьох етапів: виявлення, вирівнювання, розпізнавання.

Архітектура процесу розпізнавання обличчя зображена на рисунку 2.5.

Існує приватний інтерфейс FaceManager, який підключається до FaceService. FaceService – це інфраструктура, яка керує доступом до обладнання для розпізнавання обличчя (ідентифікації). Саме ця інфраструктура використовує ключ для доступу до ідентичності особи.

Face Unlock забезпечує високий рівень безпеки, оскільки вимагає фізичного присутності користувача перед пристроєм. Однак важливо враховувати, що цю технологію можна обдурити за допомогою фотографій обличчя або інших методів.

Сучасним прикладом використання датчика розпізнавання обличчя є домофони. Майже в кожному в багатоквартирному або приватному будинку є система домофонів, яка містить в собі чотири види ідентифікації особи:

картковий, пін-код, відбиток пальця та розпізнавання обличчя.

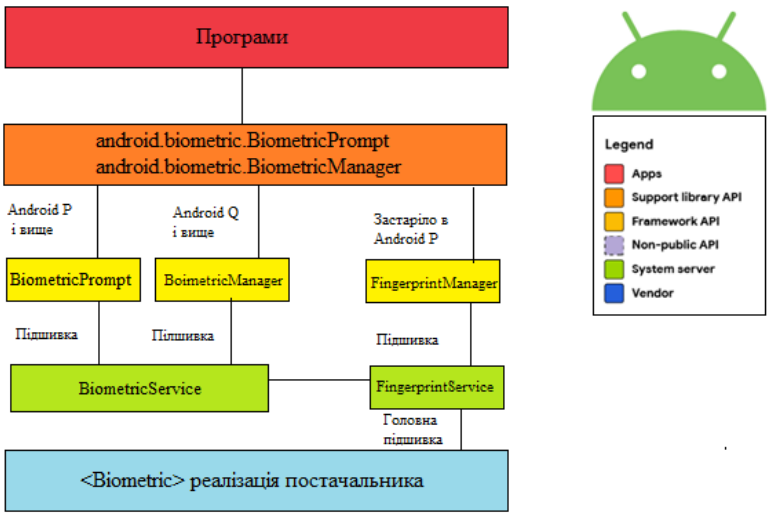

Рисунок 2.5 – Архітектура процесу розпізнавання обличчя

Рисунок 2.6 – Домофон з чотирма видами ідентифікації

Smart-домофон укомплектовано сенсорним екраном, відеокамерою та сканером для відбитків пальців. Система дозволяє обирати користувачам як потрапити в будинок: просканувати палець, обличчя, або магнітну картку, або ввести пін-код.

Отже, розпізнавання обличчя не є надійним способом ідентифікації особи, оскільки існує велика ймовірність використання фото або іншої людини (брат або сестра), на яких існує ймовірність, що сканер спрацює.

2.3 VeriEye (технологія розпізнавання райдужної оболонки ока (ірису))

Розпізнавання райдужної оболонки ока – це автоматизований метод біометричної ідентифікації, який виявляє унікальні візерунки в кільцеподібній області навколо зіниці кожного ока. Це надзвичайно надійний і точний метод ідентифікації з дуже низьким рівнем помилкових збігів.

VeriEye технологія розроблена для ідентифікації райдужної оболонки ока (ірису), включає багато рішень, які надають надійну реєстрацію ока при різних умовах і швидке розпізнавання ірису по системі «1 до 1» або «1 до багатьох».

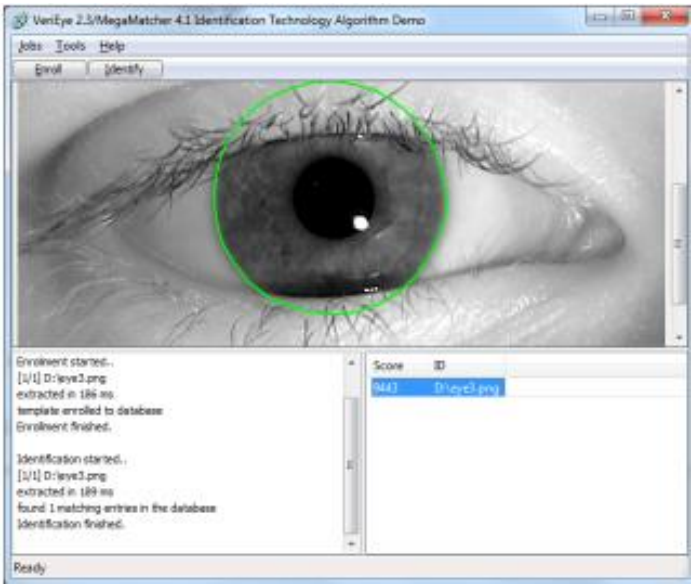

Рисунок 2.6 – Технологія VeriEye

Зв’язок «1 до 1» – одна характеристика отриманих даних має відповідати одній характеристики з чинних баз даних. Зв’язок «1 до багатьох» – до однієї характеристики з отриманих даних є відповідність

кількох характеристик з вже створених баз даних.

VeriEye доступна для розробників для автономних і мережевих рішень на різних платформах (Microsoft Windows, IOS, macOS, Android, Linux).

Реалізація вдосконаленої сегментації райдужної оболонки, реєстрації, зіставлення за допомогою алгоритмів цифрової обробки зображень. Перш за все, перевага цього методу полягає в тому, що райдужну оболонку можна виявити навіть за наявності перешкод: поганого освітлення, візуальних шумів тощо. Система автоматично стабілізує світло, піднімає повіки або видаляє непотрібні об'єкти.

Особливості технології VeriEye:

- надійне розпізнавання у будь-якому положенню ока;
- швидка ідентифікація;
- точна ідентифікація;
- виявлення живості райдужної оболонки;
- адекватні ціни на ліцензування та підтримку.

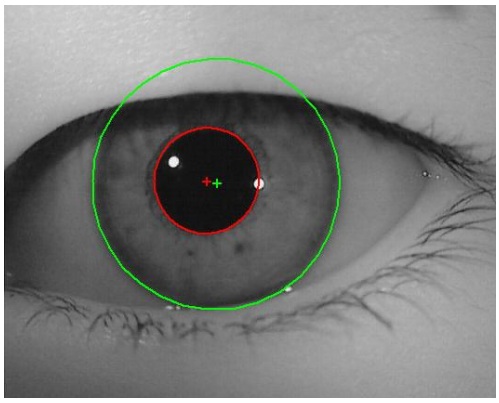

Рисунок 2.7 – Ідентифікація райдужної оболонки ока

Правильним розташуванням райдужної оболонки вважається: дана технологія моделює контур ока і не обов’язково це має бути ідеальне коло чи еліпс. На рисунку 2.7 червоним кольором риска і коло позначається центр і внутрішня межа райдужної оболонки ока. Зелена риска і коло – центр і зовнішня межа оболонки.

Перевагою VeriEye є здатність сприймати зображення при слабкому освітленні, з вузькими очима, з візуальним шумом і з очима, які дивляться в бік. Дана технологія може автоматично коригувати точні дані для ока.

Основним обмеженням є те, що дуже важко робити знімки з відстані понад пару метрів. Однак технологія все ще розвивається та вдосконалюється, тому розпізнавання райдужної оболонки ока може здійснюватися на відстані до 10 метрів.

Існує також алгоритм Даугмана, який використовує вейвлет-перетворення Габора (тип перетворення даних, що використовується для аналізу сигналу та зображення). Результатом цього типу є набір комплексних чисел, які містять інформацію про локальну амплітуду та фазу малюнка райдужної оболонки ока людини. В алгоритмах Даугмана більша частина амплітудної інформації відкидається і складається з 2048 біт інформації про фазу, що представляє картину райдужної оболонки.

Шаблон, створений за допомогою зображення райдужної оболонки, потім порівнюється з візерунками, що зберігаються в базі даних, для ідентифікації. Якщо відстань Хеммінга нижче порогового значення прийняття рішення, враховуючи високу ентропію шаблонів райдужної оболонки, робиться позитивна ідентифікація через статистично високу ймовірність того, що дві різні особи можуть випадково домовитися про таку кількість бітів.

Отже, перевагами ідентифікації особистості за біометричними характеристиками є те, що ірис – внутрішній орган кожної людини, який захищений від пошкоджень і зношення рогівкою. Також даний вид працює з контактними лінзами, окулярами для зору і сонцезахисними окулярами. Розпізнавання райдужної оболонки ока вважається найнадійнішою біометрією у світі.

Недоліки даного методу ідентифікації також існують. Багато сканерів можна обдурити, така ймовірність є, бо люди різного зросту. Тобто кожний раз потрібно з початку повністю налаштовувати висоту камери, що забирає

час. Наприклад, якщо не підстроїти правильно сканер, то під певним кутом він може зчитати зображення, думаючи що то справжня особистість.

2.4 Технологія голосового аналізу

Голосова біометрія – технологія, яка дозволяє ідентифікувати особистість за аналізом голосу, визначає конкретні характеристики людини при мовленні. Загалом існує кілька підвидів голосової біометрії, одним з яких є розпізнавання мови.

Рисунок 2.8 – Відповідність голосової біометрії

Автоматичне розпізнавання мовлення (ASR) є ключовим елементом технологій, які використовуються для інтерактивної голосової відповіді, розваг у автомобілі, екстрених служб тощо. Суть полягає в ідентифікації людської мови для подальшого виконання певної дії за допомогою цього інструменту. Наприклад, на цій технології працює віртуальний помічник Siri.

Наступний підвид – безпосередньо пряма голосова біометрія. Визначає кожну індивідуальну характеристику голосу. Кожен голос різний, тому що форма ротової порожнини, горла, манера у всіх різна. Ця технологія запам’ятовує, аналізує особливості мови та шукає кореляції для ідентифікації людини. Попередньо людина записує кілька разів для визначення унікальності та подальшого пошуку спорідненості.

Голосова аутентифікація – вид ідентифікації, який зосереджується на

унікальних голосових шаблонах особистості для надання доступу. Відносно дешевий спосіб, бо потребує пристрій для фіксування голосу та програмне забезпечення для розпізнавання та аналізу. Базується на унікальній біометрії голосу людини.

Plum Voice – компанія, яка спеціалізується на розробці програмного забезпечення для автоматизації голосового інтерфейсу. Створили набір інструментів, які надають розпізнавання голосу особистості. Технології можуть повністю замінити ідентифікацію KBA ((Knowledge-Based Authentication); це метод перевірки ідентичності особи, в якому вона відповідає на запитання, які стосуються інформації, яку тільки вона повинна знати).

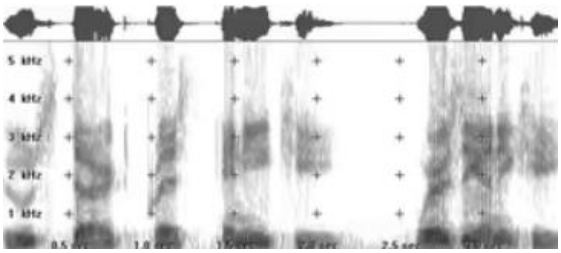

Рисунок 2.9 – Спектрограма розпізнавання голосу особистості

Недоліками розпізнавання голосу є:

- голосова біометрія не є точною;
- не захищений від записів голосу, який можуть злочинці підставити;
- наявність фонового шуму може заважати записати коректний голос особи.

2.5 Аналіз системи вен долоні або руки

Системи вен долоні або руки є найточнішою і надійною біометричною системою. Система має багато переваг:

- безконтактна технологія (фіксує зображення вен, фізично не

потрібно торкатися шкіри);

- діє тільки на живих людях;
- економічно ефективна техніка.

Даний вид біометрії найчастіше використовують великі організації, де необхідна безпека систем комп'ютерів, серверів, банківських системах, державних установах тощо. Оскільки вена людини унікальна і завдяки потужній функції розпізнавання вен майбутнє цієї технології дуже пріоритетне.

Рисунок 2.10 – Сканування вен

Розпізнавання систем вен особистості потребує NIR-камери – це камери для отримання зображень, які розроблені з певним датчиком покриття, яке може виявляти ближнє інфрачервоне світло. Перегляд вен – це система для спостереження за венами, яка використовує інфрачервоне світло, щоб заглянути під шкіру. Потім він може проектувати HD-зображення вени на поверхню шкіри.

Подвійна камера є наступним інструментом для цього методу виявлення людини. Це дві лінзи, два сенсори тощо. Основна камера працює в звичайному режимі або з невеликими змінами, як при зйомці чогось. Друга основна камера зазвичай виконує дві функції. По-перше: додайте чіткості

зображення за допомогою монохромної функції. Друге: масштабування. Іноді у двокамерній камері одна камера використовується для фотографій, а інша – для глибини різкості.

Даний тип біометрії вимагає певного положення камери та руки, які повинні бути зафіксовані таким чином, щоб зображення вени було без будь-яких шумів та перешкод, що й є недоліком.

Систему розпізнавання вен регулярно оновлюється новими технологіями та з більшою точністю. Надалі можна оновлювати пристрої з кращими характеристиками, більшою надійністю.

2.6 Технологія ідентифікації за аналізом письма

Використання письма для ідентифікації особистості з метою надійності та безпеки може здаватися нерозумним. Але використані в даному виді біометричні системи аналізують не просто форми літер, а й вони перевіряють сам процес письма: швидкість, ритм, тиск тощо. Тому використання даного методу ідентифікації можливе у багатьох сферах життя []5.

Датчики системи розпізнавання рукописного тексту можуть включати сенсорне письмо або ручку, яка включає датчики кута, тиску та орієнтації. Програмне забезпечення перетворює почерк на графік і розпізнає невеликі зміни в почерку людини.

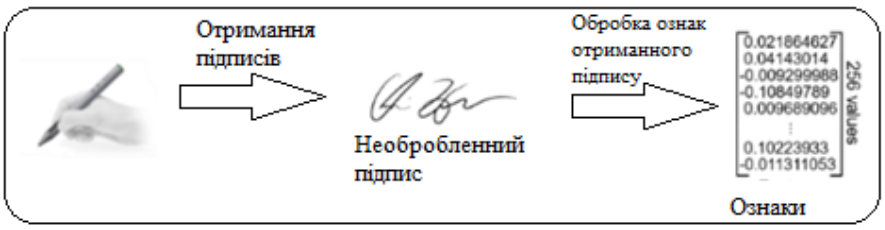

Рисунок 2.11 – Надання підпису особою для подальшої ідентифікації

На рисунку 2.11 зображено схему, яка показує спосіб обробки підпису

особи для отримання високо вимірного представлення. На рисунку 2.12 показаний сам процес перевірки, де йде порівняння підпису, який надала особистість, з тестовим підписом і підписом, який зберігається в базі даних.

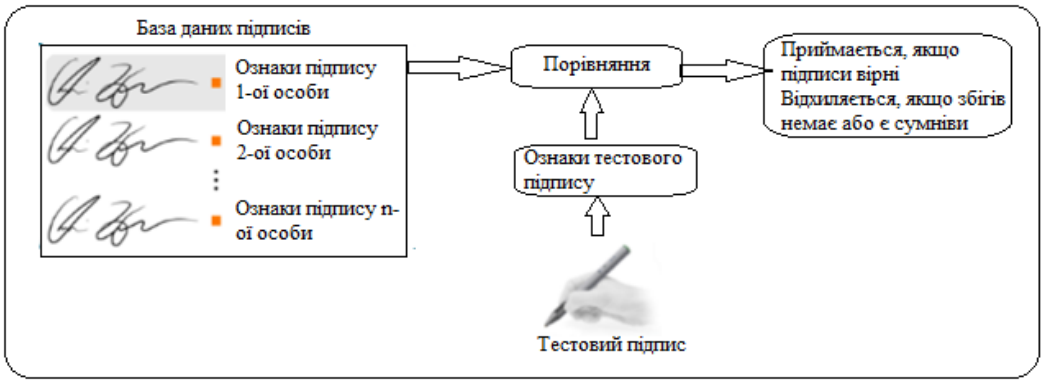

Рисунок 2.12 – Перевірка отриманого підпису та порівняння з тестовим і існуючим в базі даних

Параметри динамічного підпису описують процес створення підпису, який забезпечує більш повне та стабільне представлення. Група динамічних параметрів включає час генерації сигнатури, поверхневий тиск, нахил тощо. Ці параметри є змінними під час створення підпису, що дозволяє витягувати окремі характеристики для подальшої перевірки.

Однак правильний запис і перевірка підпису вимагає використання сумісних пристроїв, здатних записувати біометричні дані з достатньою роздільною здатністю та тиском [8]. Ці вимоги описані в ISO/IEC FDIS 19794-7 для біометричних підписів. Пізніше для цього було розроблено електронну ручку, яка зображена на рисунку 2.13.

Електронна ручка має такі характеристики:

- працює з різними пристроями;
- має датчик тиску;
- має динамік;
- має акумулятор;
- бездротова зарядка;

- BLE (Bluetooth з низкою енерговитратою);
- NFC (Near-Field Communication) для авторизації ручки в програмному забезпеченні.

Рисунок 2.13 – (а): конструкція ручки та бездротового зарядного пристрою; (б): ручка під час взаємодії з пристроєм для написання

Кожен підпис, зібраний за допомогою електронної ручки, представляється як структура даних, що містить зразки, надіслані з датчиків пристрою, і записані екранні координати кінчика пера. Точна кількість зразків координат може відрізнятися для підписів з однаковою тривалістю, оскільки підпис не фіксується, якщо кінчик пера не торкається поверхні пристрою зчитування даних.

Під час процесу ідентифікації система просить особу, яка стверджує, що є зареєстрованим користувачем, надати свій підпис (тестовий підпис). Потім згорткова нейронна мережа обробляє отриманий підпис і надсилає його на сервер ідентифікації.

Маючи як тестовий, так і основний підпис, можна обчислити евклідову відстань між ними. Оскільки мережа розроблена для обмеження вбудовування до одиничної гіперсфери, така відстань обов’язково знаходитиметься в інтервалі $\langle 0,2 \rangle$. Сервер успішно ідентифікує користувача, якщо розрахована відстань буде нижчою за попередньо визначене порогове значення.

Слід зазначити, що метод передбачає, що кожен зареєстрований користувач має один первинний підпис, пов’язаний з ним у базі даних, і один тестовий підпис для порівняння.

В алгоритмі триплетних втрат нейронна мережа оптимізується за допомогою триплетів, кожен з яких складається з двох однакових підписів. Мережа навчена таким чином, щоб кожен третій триплет не порушував умови потрійних втрат. Формула потрійних втрат визначається так:

$$l = max(0, \left|\left|A - P\right|\right|_2 - \left|\left|A - N\right|\right|_2 + \alpha, \quad (2.1)$$

де A (якір) і P (позитивні) представляють підписи, які мають бути поруч в просторі вбудовування, і N (негативний) – підпис, який відрізняється від A і P.

Слід зазначити, що A, P, і N – це вектори ознак, витягнуті нейронною мережею. Функція втрат розроблена, щоб гарантувати, що для кожного триплета відстань між A і N більше, ніж відстань між A і P з різницею α.

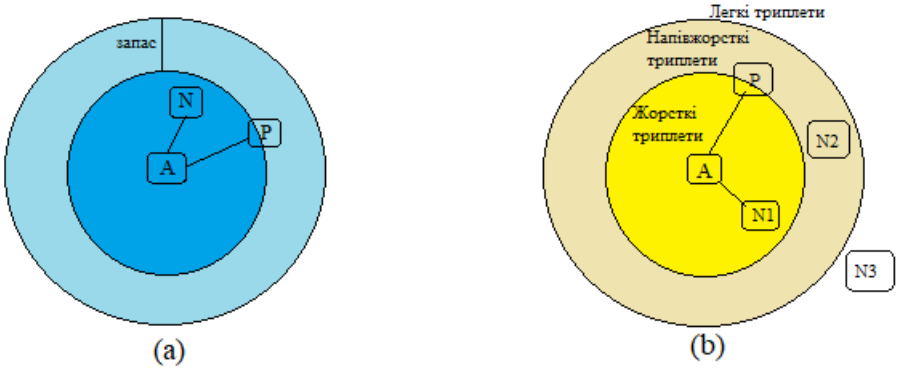

Рисунок 2.13 – (а): триплет, який порушує умову втрати триплету. A і P є вектори ознак подібних підписів. N є вектор ознак підписів, відмінної від A і P. Алгоритм триплетних втрат спрямований на те, щоб відстань від A до N (AN відстань) більше, ніж відстань AP; (б): три можливі триплети залежно від відстані між A і N

Рисунок 2.13 демонструє взаємозв'язок між елементами триплетів і показує різні типи триплетів.

Був проведений експеримент для аналізу ефективності методу, де велика кількість підписів була зібрана на ємнісному сенсорному екрані з електронною біометричною ручкою.

Кожен учасник знаходився у рівних умовах, надаючи близько п’яти зразків підписів. Завдання полягало в тому, щоб підписати послідовно в одному стилі, властивому одній людині. Однак необхідно враховувати людський фактор і помилки в наборі даних, приклади яких наведено на рисунку 2.14.

Людина 1 поставила два підписи (рис. 2.14, а, б), але в (рис. 2.14, в) написала прізвище під іменем, а не поруч. Людина 2 поставила підписи (рис. 2.14, d, e), але прізвище написала в іншому місці (рис. 2.14, f), також змінила місцями ім’я та прізвище (рис. 2.14, g). На рис. 2.14, h вказали лише ім’я. І у людини 3 на рис. 2.14, і бачимо, що поганим доторканням електронною ручкою до пристрою зчитування отримали поганий результат.

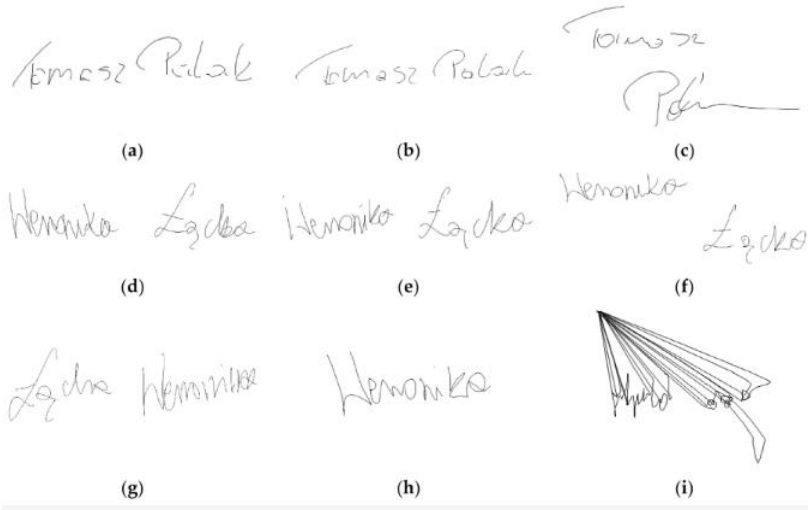

Рисунок 2.14 – Типові помилки при проведенні експерименту

Наявність помилки в наборі даних вимагає ручного очищення, щоб переконатися, що підписи кожної особи є узгодженими та що стиль підпису розглядається кілька разів.

Вибір нейронної мережі.

Кількість використаних зразків завжди постійна для створення вставки однакового розміру. Це робиться шляхом повторної вибірки кожного ряду даних із 512 вибірками за допомогою лінійної інтерполяції. Потім рука містить 512 зразків, кожна з яких містить 9 значень, тобто 4608 значень на підпис.

Перед використанням підпису як вхідних даних для нейронної мережі виконується обробка, що складається з перетворення системи координат і нормалізації зразків, зібраних з пера та екрана.

Трансформація отриманих зразків: за координатами екрана розраховується середнє положення так, щоб центр системи координат знаходився посередині руки. Кожна вибірка (x, y) потім перетворюється на полярні координати (r, θ).

Крок нормалізації ділить радіус r на максимальне значення для сигнатури, щоб він залишався в діапазоні $\langle 0,1 \rangle$. Нормалізується азимутальний кут θ із діапазону $\langle -\pi, \pi \rangle$ до $\langle -1,1 \rangle$.

Перетворення зразків біометричної ручки: перетворюються вектори акселерометра з декартових [x, y, z] вектори до сферичних [r, θ, φ] координат. Ділення радіусу на максимально можливе прискорення / кутову швидкість, яка була визначена як ±3g і ±3000°/c відповідно, щоб зберегти його значення в діапазоні $\langle 0,1 \rangle$. Азимутальний кут θ нормалізоване з діапазону $\langle -\pi, \pi \rangle$ до $\langle -1,1 \rangle$, тоді як полярний кут φ знаходиться в діапазоні $\langle 0, \pi \rangle$ до $\langle 0,1 \rangle$. Тиск пера також обмежений діапазоном $\langle 0,1 \rangle$.

Тоді кожен рядок даних містить фіксовану кількість нормалізованих вибірок у вигляді 512 ознак на 9 каналів. Сигнатура такої форми передається в нейронну мережу для створення 256-вимірного вбудовування. Найкращі результати показані на рисунку 2.15.

Замість звичайних згорткових шарів використовуються згорткові шари, що діляться по глибині, що забезпечує значне прискорення без втрати якості.

За винятком рівня перед шаром нормалізації L2, кожен такий рівень використовує функцію активації PReLU (Parametric Rectified Linear Unit). Таким чином, нахил функції активації можна оптимізувати та встановити незалежно для кожного нейрона.

Нормалізація L2 вирівнює результат попереднього шару до 256-вимірного вектора та проектує його на поверхню одиничної гіперсфери. Це робиться шляхом обчислення довжини цього вектора за допомогою евклідової метрики та ділення всіх його компонентів.

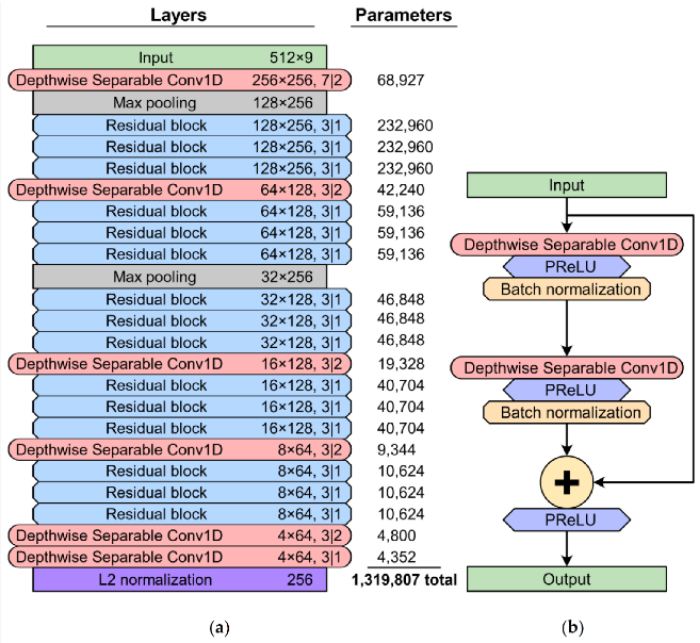

Рисунок 2.15 – (а): послідовні рівні архітектури нейронної мережі; (б): блок-схема, яка використовується як шар типу (а)

Алгоритм навчання мережі.

Для навчання мережі використовується триплетний алгоритм втрати. Тому поділяємо набір даних на 2 підмножини – навчальний набір (складається з 3064 клієнтів) і основний набір (складається з 300 клієнтів).

Навчальний набір вибирається випадковим чином з рівномірним розподілом для створення партії, що містить 256 трійок на фазі навчання. Кожен триплет сприяє оновленню градієнта, а для підтримки стабільності

зчитування використовується напівсуворий негативний аналіз. На рисунках 2.16 і 2.17 показані значення точності і втрат при навчанні нейронних мереж.

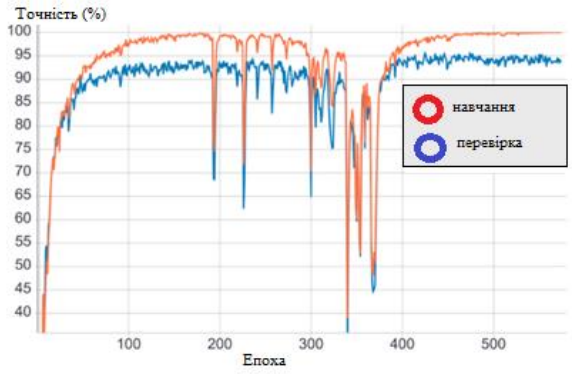

Рисунок 2.16 – Точність нейронної мережі під час навчання. Точність визначається як відсоток триплетів, які задовольняють умову запасу втрат триплетів у випадково відібраній партії з 2048 триплетів

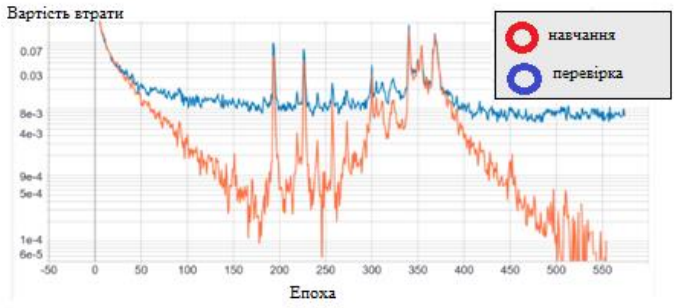

Рисунок 2.17 – Значення втрат нейронної мережі під час навчання. Приблизні втрати розраховуються для випадково відібраної партії з 2048 триплетів

Мета експерименту: порівняти пари підписів для кожної особи. Якщо вибрано дві руки, що належать одній людині, очікується, що евклідова відстань між ними буде нижче певного порогу. Крім того, пари підписів, що належали двом різним клієнтам, також порівнювалися, що дало більшу відстань, ніж обмеження.

В одному тесті було порівняно 2306 пар підписів однієї особи та 539

721 пар підписів, що належать різним клієнтам. Цей тест було повторено для 200 порогових значень, рівномірно розподілених у діапазоні $\langle 0,2 \rangle$, оскільки відстані між двома випадковими входами обмежені цим діапазоном. Мережа досягла EER (еквівалентна частота помилок) 5,94% для порогового значення 1,055. на рисунку 2.18 показана крива ROC (робоча характеристика приймача), де кожна точка відповідає одному випробуванню для заданого порогу.

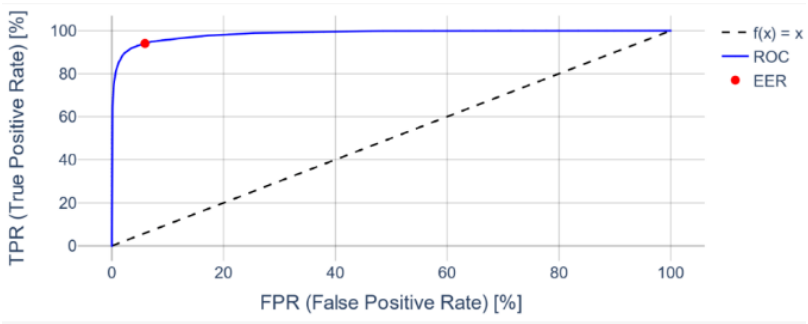

Рисунок 2.18 – Крива робочих характеристик приймача (ROC) для нейронної мережі

Таким чином, алгоритм може бути розроблений для ідентифікації користувача за допомогою нейронної мережі для вилучення значущих ознак із рукописних підписів. В експерименті використовується спеціально розроблений пристрій для біометричної перевірки.

Ефективний метод динамічної автентифікації користувача на основі підпису. Цей метод використовує триплетний алгоритм втрати для навчання моделі нейронної мережі, яку можна використовувати для вилучення значущих функцій із підписів фіксованої довжини, добре згрупованих для окремих підписів і відокремлених від інших груп підписів клієнтів.

2.7 Технологія розпізнавання ходьби

Процес ідентифікації людей за їх пересуванням (ходьба або біг)

називається розпізнавання ходи. З появою якісних методів запису ходи, наприклад, якісних камер або костюми для захоплення руху, зростає популярність даного методу ідентифікації особистості [3].

Хода людини унікальна, як і відбитки пальців, райдужної оболонки ока, голос тощо. Використовуючи ці знання, була створена технологія розпізнавання мовлення на основі алгоритмів машинного навчання (ML). Системи на основі ML можуть ідентифікувати людину на зображенні, навіть якщо обличчя людини не видно або приховано.

Система ідентифікує людину з бази даних, аналізуючи силует, зріст, швидкість і ходу. Цей метод зручніший, ніж сканування сітківки ока або сканування відбитків пальців, оскільки він менш нав'язливий.

Технологія розпізнавання жестів включає кілька записуючих пристроїв, які надають інформацію про людину – відеокамери, датчики руху тощо. Отримані дані проходять кілька етапів розпізнавання.

Основний алгоритм полягає у розпізнаванні ходу, обробленні отриманих даних (розпізнає контури, силуети, сегментує окремі риси людини) [4]. Потім алгоритм виділяє ознаки певної особи, знаходить відмінність.

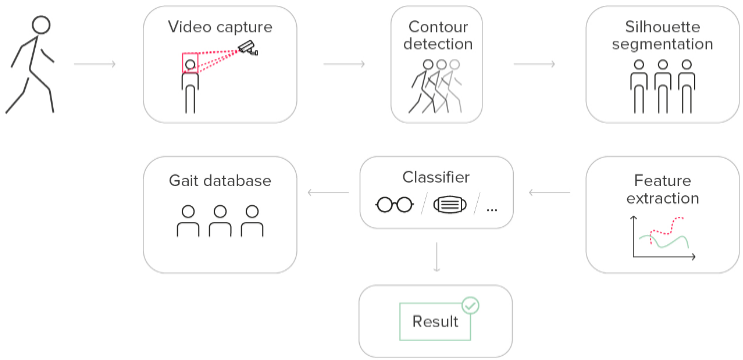

Рисунок 2.19 – Алгоритм визначення особливостей ходьби особи

Під час експерименту була зібрана база даних пересування людей, яка включає записи пересування 159 людей на різних відстанях, які були

зроблені за допомогою датчиків і камер високої чіткості. Отримані дані завантажуються в нейронну мережу для обробки зображень. Тоді розпізнавання людей у русі було майже на 100% точним. Робота системи ML заснована на принципі глибокого залишкового навчання, що дозволяє ідентифікувати людину за просторовими і часовими характеристиками її сліду.

Система розпізнавання ходи базується на:

- фіксації руху;
- сегментація силуету;
- виявлення контуру;
- виділення ознак.

Біометричні системи фіксують кроки за допомогою відеозображень, а потім перетворюють зібрані дані в математичне рівняння. На ходу як показник може впливати: взуття, місцевість, втома та травма, що є недоліком даного алгоритму.

Перевагою технології розпізнавання ходи є можливість застосування без згоди особистості. Крім того, відсоток помилок становить лише 60%.

Недоліком системи є обов’язкова наявність сенсорних панелей і камери з високою роздільною здатністю. Також система може розпізнавати лише людей, чиї дані були заздалегідь записані та збережені в базі даних.

Також існує програмне забезпечення для розпізнавання ходи – Exer Gait. Цю технологію використовують для ідентифікації людини в цілях безпеки, інколи використовують для стеження за станом здоров’я. Розпізнавання ходи є вимірюванням того, як особистість ходить або біжить на основі унікальних характеристик для ідентифікації.

Для машинного навчання були створені різні моделі вимірювання ходи. Процес відстеження, моделювання, аналізу та прогнозування моделей ходи покладається на нейронну мережу і машинне навчання. Складається процес з таких етапів:

- машинне навчання;

- згорточна нейронна мережа;
- введення даних сенсорно у вигляді фото, відео або з датчиків.

Програмне забезпечення надає можливість використовувати звичайну камеру смартфона, планшета чи комп’ютера. Ті пристрої, які можу спостерігати та фіксувати рух людини в реальному часі. І вони відносно коштовні, не потребують спеціальних технологій, що є перевагами.

Коли людина рухається, камера фіксує особливості руху та надсилає інформацію програмі машинного навчання. Курс даної особи завантажується в програмне забезпечення, за яким воно може аналізувати та ідентифікувати особу. Потім програма повертає або позитивний результат (ідентифікує особу), або негативний результат (без ідентифікації).

Тому система ідентифікації людини за ходою не є універсальною. Спочатку введіть необхідну інформацію про людину в базу даних, помістіть її в кімнату з датчиками та стежте за допомогою якісних камер. По-друге, алгоритми розпізнають лише те, що є в базі даних, тому масштабувати технологію буде більш проблематично. З іншого боку, технологія не вимагає контакту з людиною і її легко встановити для використання в громадських місцях. І частота помилок нового алгоритму не така велика.

2.8 Електрокардіограма (ЕКГ) як метод ідентифікації особи

Біометрична електрокардіограма (ЕКГ) є одним із типів характеристик для ідентифікації людини та має перевагу безпеки, оскільки базується на специфічному потенціалі серця. Тому ЕКГ можна використовувати для біометричного розпізнавання. Слід пам'ятати, що серцебиття змінюється, сигнали змінюються або залежать від фізичних навантажень, вживання поганих речовин і сильних емоцій; в цьому випадку процес ідентифікації більш складний, ніж у статичних умовах організму.

Для ідентифікації існують методи опорних точок і використання взаємозв’язків або характеристик опорних точок, таких як інтервали між

опорними точками, наприклад інтервал RR і тривалість ST-T.

Для подолання обмеженьу вигляді емоційного стану, фізичної активності тощо, запропоновано незалежні методи аналізу загальної морфології. Дослідники представили метод, заснований на відстані між першою і другою похідними сигналів.

Для індивідуальної ідентифікації за допомогою сигналів ЕКГ був розроблений багатоетапний процес для зміни необробленого сигналу ЕКГ на стандартний багатоциклового сигналу ЕКГ. Загальна діаграма для отримання сигналу багатоциклової ЕКГ показана на рисунку 2.20.

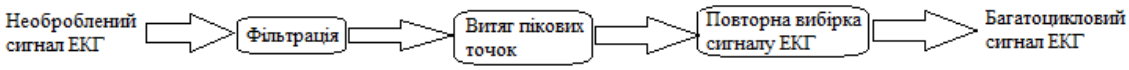

Рисунок 2.20 – Етапи процесу отримання кадру багатоциклового сигналу ЕКГ

Сигнали ЕКГ отримували за допомогою схеми вимірювання ЕКГ, плати збору даних (DAQ) і персонального комп’ютера. Схема вимірювання ЕКГ – це одноканальний аналоговий модул, який подає на вхід 5В постійного струму. Для отримання ЕКГ-сигналу на зап’ясті або пальці кріпляться три електроди.

На виході ЕКГ спостерігалися шуми потужності та високочастотні шуми. Ці шуми були видалені за допомогою смугового фільтра з діапазоном частот від 0,3Гц до 35Гц, і вони були реалізовані в аналоговому режимі.

В якості обмежувача для класифікації стандартної рамки сигналів ЕКГ були обрані позитивні високі пікові точки, які є найбільш помітними точками, які безпомилково виявляються навіть у зашумлених сигналах.

Другий найвищий позитивний пік можна легко знайти шляхом обчислення диференціювання заданого циклу зазначеного сигналу між 50 вибірками.

Перевірка чотирьох алгоритмів зіставлення шаблонів, тобто косинусної подібності, крос-кореляції, міської квартальної відстані та евклідової відстані, виглядає наступним чином.

Косинусна подібність вимірює подібність між двома векторами як простір скалярного добутку, який обчислює косинус кута між ними. Його можна виразити як скалярний добуток на величину двох векторів:

$$d_{cos}(A,B) = \frac{A*Б}{||A||_{||B||}} = \frac{\sum_i^H A_i * B_i}{\sqrt{\sum_i^H (A_i)^2}\sqrt{\sum_i^H (B_i)^2}}, \quad (2.2)$$

де N – кількість зразків, A – навчальні дані, B – тестові дані. Сигнал із найвищим значенням оцінки вибирається як найбільш схожий із вхідним сигналом.

Перехресна кореляція – це міра подібності двох послідовних сигналів як функція відставання одного відносно іншого. Перехресні кореляції корисні для визначення часової затримки між двома сигналами, тоді як вибіркові перехресні кореляції використовуються для визначення ступеня подібності між вхідним сигналом і сигналом бази даних.

Евклідова відстань – це довжина відрізка, що сполучає дві точки. Використовується для пошуку найбільш схожих сигналів із вхідним сигналом за допомогою наступного рівняння:

$$d_{euclideon}(A,B) = \sqrt{\sum_{i=1}^{H}(A_i - B_i)^2}, \quad (2.3)$$

Мета зіставлення шаблонів у дослідженні полягала в ідентифікації особи в наборі тестових даних шляхом знаходження мінімальної відстані для шаблону в наборі навчальних даних. Також було протестовано цикл роботи з одним сигналом для визначення ефекту узгодження шаблону вимірювання з

існуючими.

На рисунку 2.21 зображено накладення сигналів ЕКГ для трьох різних осіб. Патерни хвиль відрізнялися між суб'єктами. Ця тенденція означає, що зіставлення ЕКГ можна використовувати для ідентифікації людей.

Коефіцієнт ідентифікації I як міра оцінки розраховується наступним чином:

$$l = \sum_i x_i / H, \tag{2.4}$$

де x і дорівнює 1 або 0 залежно від того, чи правильно ідентифікований і -й тестовий зразок ЕКГ для його суб'єкта, а N - загальна кількість тестових зразків.

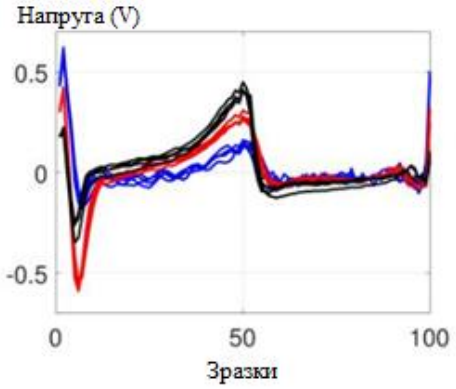

Рисунок 2.21 – ЕКГ від трьох різних осіб

Таблиця 2.1 – Показники ідентифікації за чотирма різними методами зіставлення шаблонів з використанням даних ЕКГ зап’ястя для 55 суб’єктів.

Довжина сигналу	Косинус	Хрестик	Міський квартал	Евклідова відстань
Один цикл	78 %	83 %	86 %	89 %
Два цикли	85 %	85 %	89 %	90 %
Три цикли	86 %	86 %	93 %	93 %

За результатами підтверджено, що запропонований метод може бути використаний для ідентифікації особистості. Рівень ідентифікації з мірою евклідової відстані склав 93%. Цей метод показав найвищий показник ідентифікації.

Рівень ідентифікації за мірою косинусної подібності становив 89%; мав найгіршу продуктивність серед протестованих методів. Вимірюючи міські квартали, точність зросла до 90%.

Метод із використанням сигналів із трьома тактами працював краще, ніж використання сигналів з одним або двома тактами, незалежно від алгоритмів узгодження. Багатоциклічні сигнали надали кращу інформацію для класифікації ЕКГ.

Сучасне обладнання, що використовується для вимірювання сигналу ЕКГ, звичайно, просте для отримання стабільного та повторюваного сигналу; однак запропонований метод, який відповідає стандартній структурі ЕКГ-сигналів, дозволяє спостерігати характеристики окремих серцевих сигналів, які можуть бути використані як альтернативний захід ідентифікації людини. Однак слід враховувати, що різні стани організму, хвороби серця тощо можуть давати помилкові показники.

Отже, всі методи ідентифікації мають як переваги, так і недоліки. Тому, гібридизація методів є рішенням для уникнення значних недоліків: підробки біометричних характеристик, не точніть через забруднення пальці та інші фактори, що можуть впливати на якість ідентифікації.

3 ГІБРИДИЗАЦІЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА БІОМЕТРИЧНИМИ ДАНИМИ

3.1 Види гібридизації методів ідентифікації особи за біометричними даними

Гібридизація методів полягає в поєднанні двох або більше методів ідентифікації людини за біометричними даними для досягнення найкращого результату в певній сфері. Існує кілька видів гібридизації, які найчастіше використовуються в різних системах, а також більш ефективні та безпечні [13].

Одним із найпоширеніших видів гібридизації є багатосенсорні системи. Суть методу полягає в тому, що за допомогою різних датчиків збираються біометричні характеристики людини. Наприклад, камери, датчики відбитків пальців, мікрофони тощо. Поєднання декількох датчиків дозволяє підвищити точність отриманих даних для подальшої ідентифікації людини.

Приклад використання багатосенсорної системи: віртуальна реальність (Virtual Reality) та доповнена реальність (Augmented Reality), які використовують сенсори для аналізу рухів, жестів особи і т.д. В кібербезпеці даний вид гібридизації дає можливість відслідковувати загрози в комп’ютерних мережах завдяки датчикам, які моніторять різні аспекти безпеки (мережевий трафік, поведінку користувача тощо).

Також існує мультимодальний вид гібридизації біометрії, який є зв’язуючим етапом кількох методів ідентифікації. Прикладом є відбитки пальців і голосова біометрії. Підхід забезпечує точність та надійність вище, ніж у випадку використання одно з видів ідентифкації.

Мультимодальна біометрія поєднує відбитки пальців і розпізнавання голосу; відбитки пальців і розпізнавання обличчя; розпізнавання ірису і обличчя; сканування відбитків пальців, розпізнавання голосу і розпізнавання

вен долоні. Перевагою даного виду гібридизації є покращення точності та надійності ідентиіфкації особи завдяки зчитуванню різних характеристик людини. Використовується в багатьох сферах, таких як кібербезпека, медицина, банки тощо.

Наступний вид гібридизації є динамічним і містить в собі динамічні параметри (ходьба, рух очей, підпис) та їх використання разом зі статичними даними. Даний вид ідентифікації складно підробити, тому вважається більш-менш безпечним.

Системи відрізняються від статичних тим, що вони використовують динаміку в часі, що є відмінним. Приклади динамічних біометричних систем:

- рухи очей (швидкість, шлях руху);
- відбитки пальців (система враховує рух під час сканування);
- голос (швидкість, тембр, інтонація тощо);
- руки (жести);
- ходьба (стиль, швидкість тощо).

Комбінація біометричних методів та звичайних паролів, пін-кодів, –це є додатковим рівнем безпеки в разі втрати даних для ідентифікації особи. Так як метод являє собою перевірку особи на знання пароля і відповідність по біометричним характеристикам.

Перевагами даного методу є зручність для користувача, тому що можна обрати зручніший метод для ідентифікації. Також безпечність і зменшення ризику підробки. Комбінація кількох методів може створювати двофакторну аутентифікацію, де всі використані методи повинні бути підтвердженні.

Фузія біометричних даних для ідентифікації особистості – це об’єднання різних біометричних методів задля створення повноцінної системи ідентифікації. Являє собою комбінацію даних з різних джерел, які зчитують біометричні дані (сенсори, фото або відео спостереження і т.д.).

Існує безліч різних алгоритмів фузії, які використовуються для об’єднання інформації з різних джерел:

- фузія рішень – це об’єднання рішень, прийнятих гібридної системою

на основі біометричних методів (рішення приймається на основі сканування відбитків пальців і обличчя);

- фузія рішень на рівні рішень – система визначає наприкінці ідентифікації, які краще методи використовувати (наприклад, краще використовувати відбитки пальців і розпізнати обличчя. Або відбитки пальців та розпізнати ірис, так як на обличчі особи є пошкодження, які можуть заважати точному рішенню системи щодо ідентифікації);

- фузія рішень на рівні ознак – поєднує ознаки, які беруться з різних біометричних методів (наприклад, голосова біометрія і розпізнавання обличчя);

- ранжування методів полягає у оцінюванні кожного біометричного методу, на основі чого система визначає які краще використовувати для ідентифікації особистості;

- фільтрації – прибирання з ідентифікації непотрібних та невисокоефективних біометричних ознак, наприклад, погане зображення при скануванні обличчя.

Захист від фальсифікації полягає у використанні антивібиткових та антивідризнювальних технологій для захисту біометричних систем від атак або підробки. Фальсифікація означає спробу обману системи. Існують такі методи захисту від фальсифікації:

- мультимодальність (використання кількох біометричних методів);

- використання унікальних біометричних методів (наприклад, розпізнавання вен використовують досить рідко);

- шифрування біометричних даних;

- моніторинг дій користувачів (може допомогти уникнути мережевих атак і т.д.).

Отже, біометрія – це набір показників, що фіксують фізіологічні та поведінкові характеристики людини, і все частіше прийнято використовувати для програм перевірки особи. Вона охоплює широкий спектр сфер застосування, включаючи медицину, питання імміграції, офісну роботу тощо.

Дослідження з використанням біометричних характеристик показали, що забезпечення надійності, безпекою даних потрібно вирішувати у бідь-якій сфері використання. Тому гібридизація методів може покращити і вирішити деякі недоліки використання окремих біометричних характеристик для ідентифікації особистості.

Отже, на основі результатів щодо аналізу використання біометричних характеристик для створення методу гібридизації зробили поєднання біометричних характеристик на основі мультимодального методу, який було розглянуто у підрозділі 3.1.

3.2 Гібридизація методів для безпечної ідентифікації особистостей

В сучасному цифровому середовищі біометричні дані можуть бути підроблені задля несанкціонованої ідентифікації особи. Тому для більш безпечної, надійної та швидкої ідентифікації було розроблено метод гібридизації, який передбачає поєднання кількох біометричних характеристик, їх аналіз і результат.

Програмні методи, які потребують високого рівня безпеки, як правило, мають більше вимог до ідентифікації особистості з біометричними характеристиками. Тому що в разі відхилення справжнього користувача, виникають незручності, які затримують особу або викликають недовіру до компанії. У разі ж якщо система помилково ідентифікує самозванця, це може викликати серйозні проблеми. Таким чином помилкове визнання є біості системи, ніж помилкова відмова у доступі [15].

Запропоновано рішення, в основі якого використовується система, яка гібридно поєднує в собі кілька методів зчитування біометричних характеристик, а саме: сканер для відбитків пальців та фотокамера для фіксування ірису (райдужної оболонки ока).

Дві різні біометрії, ірис та відбиток пальця, розглядається як розробка для біометричної системи, яка безпечно може ідентифікувати особистість.

Запропонований метод передбачає наявність процесору, який може обробляти дані, як лише з одного пристрою зчитування, так і з двох паралельно в залежності від сфери використання та можливо виникнених проблем при ідентифікації.

Функція методу полягає у використанні бібліотек зчитування відбитків пальців (FingerPrint Sensor Library) і райдужної оболонки ока (IrisGuard SDK) [14]. Поєднання бібліотек робить метод більш універсальним, дає непогані результати роботи по часу, точність ідентифікації тощо.

Бібліотека зчитування відбитків пальців (FingerPrint Sensor Library) є програмним компонентом, який в гібридному методі існує для взаємодії користувача і системи зчитування біометричних характеристик. Містить наступні компоненти: плата Arduino, USB кабель, оптичний модуль зчитування відбитків пальців, з'єднувальні дроти. Забезпечує такі функції:

– ініціалізація датчика відбитків;
– зчитування;
– порівняння;
– фінальний результат обробки відбитків.

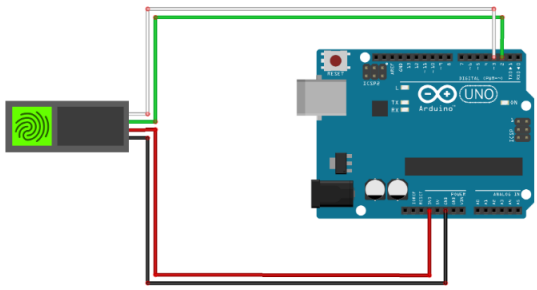

Рисунок 3.1 – Схема FingerPrint Sensor Library

Лістинг 3.1 є файлом конфігурації для набору тестів адаптера датчика. Він визначає набір тестів для запуску, бібліотеку для використання та інформацію про пристрій зчитування.

Лістинг 3.1 – Файл конфігурації адаптера датчика відбитків пальців

```
<?xml version="1.0" encoding="utf-8"?>
<bioTestConfiguration version="0" runOptional="false"
runInteractive="true" abortOnFailure="false" manualStep="false"
logType="WTT">
  <testSuites>
    <testSuite deviceRequired="true"
id="SensorAdapterTestSuite">
      <library>sensortest.dll</library>
      <description>Sensor Adapter Test Suite</description>
    </testSuite>
  </testSuites>
  <deviceInfo>
    <sensorAdapterLib>winbiosensoradapter.dll</sensorAdapterLib>
    <engineAdapterLib>engineadapter.dll</engineAdapterLib>

<storageAdapterLib>winbiostorageadapter.dll</storageAdapterLib>
    <indicatorSupported>0</indicatorSupported>
    <supportedModes>
      <supportedMode>0x01</supportedMode>
      <supportedMode>0x02</supportedMode>
    </supportedModes>
    <supportedPurposes>
      <supportedPurpose>0x01</supportedPurpose>
      <supportedPurpose>0x02</supportedPurpose>
      <supportedPurpose>0x04</supportedPurpose>
      <supportedPurpose>0x08</supportedPurpose>
      <supportedPurpose>0x10</supportedPurpose>
      <supportedPurpose>0x80</supportedPurpose>
    </supportedPurposes>
  </deviceInfo>
</bioTestConfiguration>
```

Нижче представлений файл XML є файлом конфігурації для набору тестів адаптера двигуна. Він визначає набір тестів для запуску, бібліотеку для використання та інформацію про процес обробки отриманих відбитків пальців.

Лістинг 3.2 – Файл конфігурації адаптера обробника відбитків пальців

```
<?xml version="1.0" encoding="utf-8"?>
<bioTestConfiguration version="0" runOptional="false"
runInteractive="true" abortOnFailure="false" manualStep="false"
logType="WTT">
  <testSuites>
    <testSuite deviceRequired="true"
```

Продовження лістингу 3.2

```
id="EngineAdapterTestSuite">
      <library>enginetest.dll</library>
      <description>Engine Adapter Test Suite</description>
    </testSuite>
  </testSuites>
  <deviceInfo>
    <sensorAdapterLib>winbiosensoradapter.dll</sensorAdapterLib>
    <engineAdapterLib>engineadapter.dll</engineAdapterLib>

<storageAdapterLib>winbiostorageadapter.dll</storageAdapterLib>
    <indicatorSupported>0</indicatorSupported>
    <engineOnDevice>FALSE</engineOnDevice>
    <supportedModes>
      <supportedMode>0x01</supportedMode>
      <supportedMode>0x02</supportedMode>
    </supportedModes>
    <supportedPurposes>
      <supportedPurpose>0x01</supportedPurpose>
      <supportedPurpose>0x02</supportedPurpose>
      <supportedPurpose>0x04</supportedPurpose>
      <supportedPurpose>0x08</supportedPurpose>
      <supportedPurpose>0x10</supportedPurpose>
      <supportedPurpose>0x80</supportedPurpose>
    </supportedPurposes>
  </deviceInfo>
</bioTestConfiguration>
```

Файл XML описаний у лістингу 3.3 визначає, як буде запускатися набір тестів адаптера зберігання. Він вказує, який набір тестів запускати, яку бібліотеку використовувати для взаємодії з пристроєм і яку інформацію про пристрій використовувати для тестування.

Лістинг 3.3 – Файл конфігурації адаптера сховища відбитків пальців

```
<?xml version="1.0" encoding="utf-8"?>
<bioTestConfiguration version="0" runOptional="false"
runInteractive="true" abortOnFailure="false" manualStep="false"
logType="WTT">
  <testSuites>
    <testSuite deviceRequired="false" id="StorageAdapter">
      <library>storagetest.dll</library>
      <description>Storage Adapter Test Suite</description>
    </testSuite>
  </testSuites>
  <deviceInfo>
    <sensorAdapterLib>winbiosensoradapter.dll</sensorAdapterLib>
    <engineAdapterLib>engineadapter.dll</engineAdapterLib>
```

Продовження лістингу 3.3

```
<storageAdapterLib>winbiostorageadapter.dll</storageAdapterLib>
    <indicatorSupported>0</indicatorSupported>
    <storageOnDevice>FALSE</storageOnDevice>
    <supportedModes>
      <supportedMode>0x01</supportedMode>
      <supportedMode>0x02</supportedMode>
    </supportedModes>
    <supportedPurposes>
      <supportedPurpose>0x01</supportedPurpose>
      <supportedPurpose>0x02</supportedPurpose>
      <supportedPurpose>0x04</supportedPurpose>
      <supportedPurpose>0x08</supportedPurpose>
      <supportedPurpose>0x10</supportedPurpose>
      <supportedPurpose>0x80</supportedPurpose>
    </supportedPurposes>
  </deviceInfo>
</bioTestConfiguration>
```

Iris SDK – бібліотека зчитування райдужної оболонки ока (ірис), яку можна використовувати на різних платформах. Складається з двох основних компонентів: пристрій зчитування, який використовується в гібридній системі, та програмне забезпечення. Бібліотека містить функції:

- ініціалізації сенсора;
- зчитування;
- порівняння;
- результат.

Лістинг 3.4 – Файл конфігурації адаптера датчика для ірису ока

```
import cv2
import numpy as np

def configure_iris_sensor_adapter(adapter):
    # Задаем разрешение изображения
    adapter.set_resolution(640, 480)

    # Задаем частоту кадров
    adapter.set_frame_rate(30)

    # Включаем автофокус
    adapter.enable_autofocus()
```

Продовження лістингу 3.4

```
    # Включаем подсветку
    adapter.enable_illumination()


# Создаем адаптер датчика зчитування ірису ока
adapter = cv2.IrisSensorAdapter()

# Конфигурируем адаптер
configure_iris_sensor_adapter(adapter)

# Запускаем захват изображения
adapter.start_capture()

# Получаем изображение
frame = adapter.get_frame()

# Выводим изображение
cv2.imshow("Iris image", frame)
cv2.waitKey(0)

# Останавливаем захват изображения
adapter.stop_capture()
```

Лістинг 3.4 описує процес створення адаптера датчика зчитування райдужної оболонки ока, далі конфігурацію, запуск і отримання зображення, відображення на пристрої зчитування. Функція configure_iris_sensor_adapter конфігурує адаптер датчика зчитування ірису, задаєроздільну здатність, частоту та автофокус.

Далі створюється адаптер обробника зображень (лістинг 3.5). Функція configure_iris_sensor_adapter задає порогове значення для сегментації ірису, розмір ядра для фільтра Гаусса та порогове значення для видалення шуму. Аналогічно у лістингу 3.6 створений адаптер сховища отриманих даних з райдужної оболонки ока.

Лістинг 3.5 – Файл конфігурації адаптера обробника для ірису ока

```
import cv2
import numpy as np

def configure_iris_processor_adapter(adapter):
    # Задаем пороговое значение для сегментации радужной
оболочки глаза
```

Продовження лістингу 3.5

```
    adapter.set_threshold(127)

    # Задаем размер ядра для фильтра Гаусса
    adapter.set_gaussian_kernel_size(5)

    # Задаем пороговое значение для удаления шума
    adapter.set_noise_threshold(10)


# Создаем адаптер обработчика ірису ока
adapter = cv2.IrisProcessorAdapter()

# Конфигурируем адаптер
configure_iris_processor_adapter(adapter)

# Получаем изображение радужной оболочки глаза
iris_image = adapter.process_frame(frame)

# Выводим изображение радужной оболочки глаза
cv2.imshow("Iris image", iris_image)
cv2.waitKey(0)
```

Багатопотоковий процес створює два потоки: перший – для сканування відбитків пальців, другий – для сканування райдужної оболонки ока. Потоки запускаються, аналізують отриманні біометричні характеристики і надають результат, де ідентифікація успішна або не успішна.

Лістинг 3.6 – Файл конфігурації адаптера сховища для ірису ока

```
import cv2
import numpy as np

def configure_iris_storage_adapter(adapter):
    # Задаем путь к каталогу для хранения изображений радужной
оболочки глаза
    adapter.set_storage_path("/path/to/storage/directory")

    # Задаем формат файлов для хранения изображений радужной
оболочки глаза
    adapter.set_file_format(".jpg")


# Создаем адаптер сховища для ірису ока
adapter = cv2.IrisStorageAdapter()

# Конфигурируем адаптер
configure_iris_storage_adapter(adapter)
```

Продовження лістингу 3.6

```
# Сохраняем изображение радужной оболочки глаза
adapter.save_iris_image(iris_image)
```

Лістинг 3.7 – Багатопотоковий процес аналізу отриманих біометричних характеристик

```
import threading
import time

from fingerprint_scanner import FingerprintScanner
from iris_scanner import IrisScanner
from database import Database


class IdentificationProcess:

    def __init__(self, fingerprint_scanner: FingerprintScanner,
iris_scanner: IrisScanner, database: Database):
        self.fingerprint_scanner = fingerprint_scanner
        self.iris_scanner = iris_scanner
        self.database = database

    def identify(self, biometric_data):
        # Створюємо два потоки: один для сканування відбитків
пальців, а інший - для сканування райдужної оболонки ока.
        fingerprint_thread =
threading.Thread(target=self._scan_fingerprint,
args=(biometric_data,))
        iris_thread = threading.Thread(target=self._scan_iris,
args=(biometric_data,))

        # Запускаємо потоки
        fingerprint_thread.start()
        iris_thread.start()

        # Чекаємо, поки потоки завершаться
        fingerprint_thread.join()
        iris_thread.join()

        # Отримуємо результати сканування
        fingerprint_results = self.fingerprint_scanner.results
        iris_results = self.iris_scanner.results

        # Перевіряємо, чи співпадають результати сканування з
будь-якими записами в базі даних
        match = False
        if fingerprint_results:
            match =
self.database.match_fingerprint(fingerprint_results)
```

Продовження лістингу 3.6

```
        if not match and iris_results:
            match = self.database.match_iris(iris_results)

        # Повертаємо результат ідентифікації
        return match

    def _scan_fingerprint(self, biometric_data):
        # Скануємо відбитки пальців
        self.fingerprint_scanner.scan(biometric_data)

    def _scan_iris(self, biometric_data):
        # Скануємо райдужну оболонку ока
        self.iris_scanner.scan(biometric_data)


if __name__ == "__main__":
    # Створюємо сканер відбитків пальців та сканер райдужної
оболонки ока
    fingerprint_scanner = FingerprintScanner()
    iris_scanner = IrisScanner()

    # Створюємо базу даних
    database = Database()

    # Створюємо об'єкт процесу ідентифікації
    identification_process =
IdentificationProcess(fingerprint_scanner, iris_scanner,
database)

    # Скануємо дані біометрії
    biometric_data = "1234567890"
    match = identification_process.identify(biometric_data)

    # Виводимо результат ідентифікації
    print(match)
```

Гібридне поєднання методів ідентифікації є наступним: база даних з біометрією певних користувачів, яка була створена заздалегідь, куди були додані біометричні зразки. Також є дві частини бібліотек гібридної системи, які працюють паралельно або послідовно в залежності від задач.

Вважається, що райдужна оболонка ока є більш надійною та безпечною, її неможливо підробити та пошкодити. Тому система з використанням технології VeriEye для ідентифікації виглядає наступним чином: людина, яку потрібно ідентифікувати, підходить до зчитувача ірису –

фотокамери, яка фіксує око.

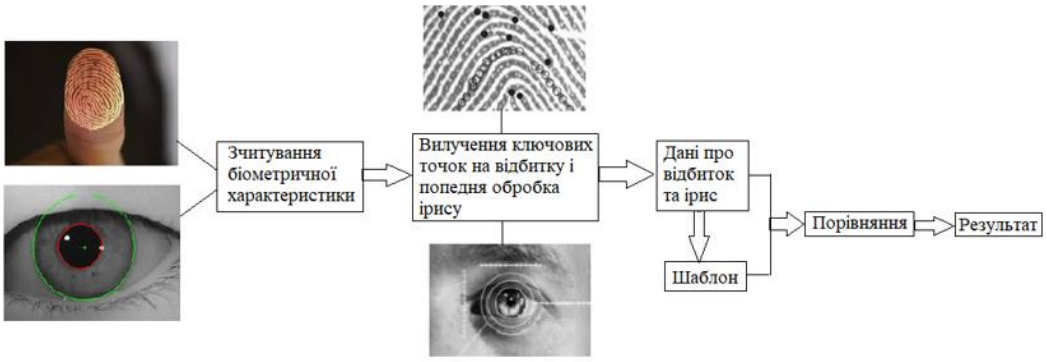

Рисунок 3.2 – Запропонована схема гібридної системи для ідентифікації особи за біометричними характеристиками

Обробка отриманого ірису полягає у прибиранні шумів, корекції світла, і враховуючи всі недоліки отриманого фото, система обробляє і висвітлює райдужну оболонку ока. Пристрій запам’ятовує її та система по рангам починає порівнювати отриманий ірис з вже наявними в базі даних. Ідентифікація людини визначається відповідно до його рангу в двох або більше матчів, щоб надати остаточний результат обробки. Архітектура гібридної системи зображена на рисунку 3.3.

Перевірка пройшла успішно на цьому етапі, тож необхідний доступ для ідентифікації буде надано, і процес буде припинено. Якщо перевірка одного зразку на першому етапі не збігається з наявними біометричними характеристиками в базі даних, то починає послідовно працювати друга частина системи по такому ж самому принципу.

В іншому випадку, за райдужною оболонкою гібридна система не ідентифікувала особистість, то сканується відбиток пальця. Сканер з високою роздільною здатністю, має багато струмопровідних частин, яких торкається палець при збору відбитків. Відповідно при дотику пальцем сканеру заряд, який знаходиться в конденсаторі, відтворює відбиток з усіма особливостями. Після чого система так само порангами перевіряє відповідність.

В залежності від відповіді системи користувач буде ідентифікован або ні.

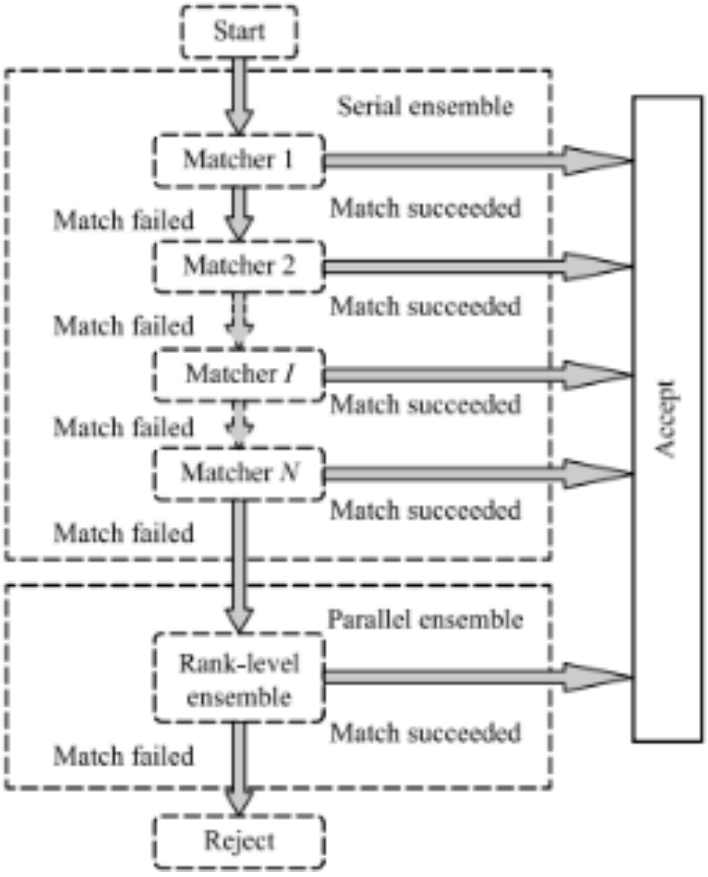

Рисунок 3.3 – Архітектура перевірки біометричних характеристик

В разі використання нашого гібридного методу в значиних установах, де безпека має найвищу пріоритетність, то є можливість паралельно перевіряти дві біометричні характеристики.

Для оцінки запропонованої структури гібридизації, проводяться деякі дослідження з використанням відбитків пальців і райдужної оболонки ока в послідовній обробці та паралельній.

Мультимодальний вид гібридизації біометрії базується на ідеї того, що використання кількох біометричних параметрів одночасно може знизити ризик помилкової ідентифікації. Такі системи можуть використовувати різні види біометричних даних, такі як відбитки пальців, розпізнавання обличчя,

розпізнавання голосу, ходьби та інші. Наприклад, система може вимагати одночасного вводу відбитку пальця та розпізнавання обличчя для підтвердження особи.

Мультимодальні системи біометрії дозволяють підвищити надійність ідентифікації та зменшити ймовірність помилок. Однак ці системи можуть бути витратними та складними у впровадженні, оскільки вони вимагають обладнання та програмного забезпечення для збору і аналізу різних видів біометричних даних.

4 ДОСЛІДЖЕННЯ МЕТОДУ ГІБРИДИЗАЦІЇ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА БІОМЕТРИЧНИМИ ДАНИМИ

4.1 Тестування гібридної системи

Для оцінки ефективності методу було проведено експеримент, де залучено 100 осіб. У яких отримали біометричні характеристики для подальшої ідентифікації.

Було проведено три етапи перевірки біометричних характеристик. В першому зразку зі ста осіб зібрали відбитки пальців. Після чого система проаналізувала та ідентифікувала 95 особистостей, тобто 5 – отримали відмову. Процес від зчитування відбитків пальців до відповіді системи без перешкод зайняв 8 секунд. У деяких осіб були забруднення на пальцях, тож аналіз відбувся за 15,2 секунд. Після холодної погоди пальці були замерзлі, тож сканер досить довго не міг відсканувати, що в підсумку зайняло 20,9 секунд. Точність виконаної ідентифікації складає 96%, так як серед осіб були самозванці. Результати першого експерименту занесені в таблицю 2.

Наступним експериментом є ідентифікація особи за райдужною оболонкою ока (ірисом). Система зібрала у певної кількості осіб біометрію ірису і отримали результати: 2 особи не було ідентифіковано. Відповідно 98 осіб ідентифіковано. В гарних умовах людей система ідентифікувала за 20 секунд. І були випадки з шумом і поганим освітленням, тоді витрачено було близько 38,4 секунд на одну людину. При цьому серед самозванців система помилково ідентифікувала лише 2 людини, тому виходить 98% – точність ідентифікації за райдужною оболонкою ока. Результати занесені в таблицю 2.

Третій етап – використання двох біометричних характеристик (відбиток пальця і райдужна оболонка ока) для ідентифікації особистостей. В даному випадку, 13 осіб зі 100 отримали відмову при ідентифікації. Час для аналізу біометрії та отримання відповіді системи зайняв досить багато часу.

При нормальних умовах, без перешкод – 48 секунд. З перешкодами: забруднення на пальцях, погане освітлення тощо, – 87,3 секунди. Проте, точність ідентифікації була 99%. Так як при процесі ідентифікації самозванця за відбитками пальця система надала позитивний результат. Але з ірисом відповідь була негативною. Тому гібридна система ідентифікації має досить велику точність.

Таблиця 4.1 – Результати експерименту

	Загальна кількість осіб	Кількість часу ідентифікації (без перешкод / з перешкодами) (сек)	Ідентифікація вірна	Ідентифікація невірна (самозванця)	Точність ідентифікації (%)
Відбиток пальця	100	8 15,2	95	5	96
Райдужна оболонка ока (ірис)	100	20 38,4	98	2	98
Відбиток пальця + райдужна оболонка ока	100	48 87,3	87	13	99

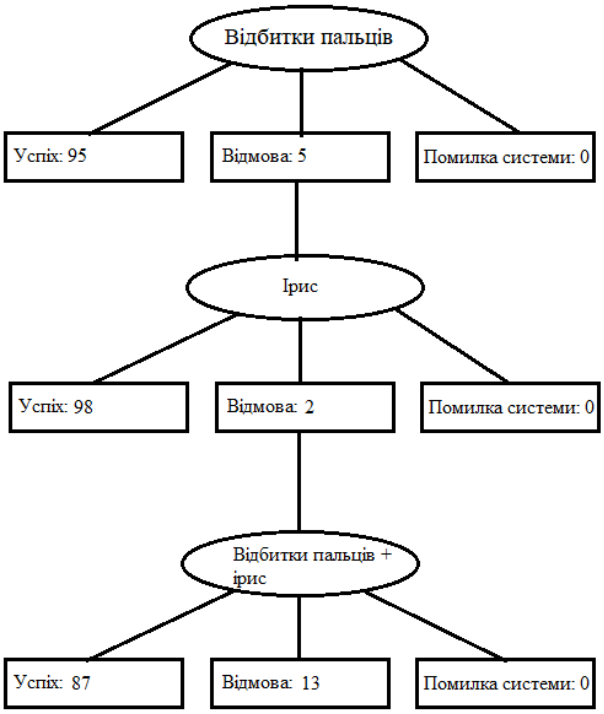

Рисунок 4.1 – Кількість розпізнавання біометрії

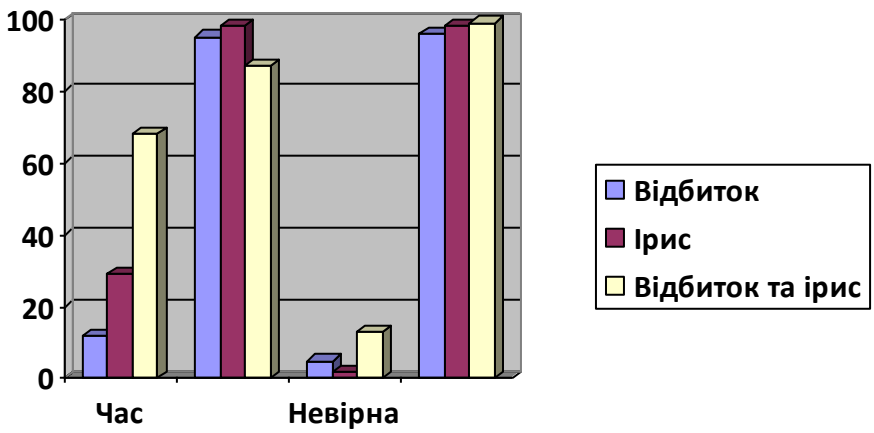

Рисунок 4.2 – Діаграма результатів експерименту

Отже, можна зробити висновки, що гібридизація методів ідентифікації особистостей за біометричними характеристиками має переваги в точності ідентифікації. Використовуючи декілька біометричних характеристик

система надасть точні результати, безпомилкових ідентифікацій. Глобальною перевагою є покращення точності та надіцності ідентифікації особистостей. Одже використання кілької біометричних характеристик мають більш безпечний захист, так як біометрія людини має слабкі сторони. Наприклад, відбиток пальця та ірис може змінитися в результаті поранення і тоді ідентифікувати людину значно складніше. Гібридні системи ідентифікації можуть компенсувати слабкі сторони одного біометричного параметра за рахунок сильних сторін іншого.

Другою перевагою є рівень безпеки з боку підробки також більший у гібридних системах, тому що потенційна особа для ідентифікації повинна надати кілька біометричних характеристик. Це може бути проблемою для особи, яка хоче отримати несанкційований доступ до будь-яких особистих даних.

ВИСНОВКИ

В кваліфікаційній роботі була поставлена задача гібридизації методів ідентифікації особистостей за біометричними характеристиками для покращення надійності та безпеки особистих даних. Проведений аналіз існуючих рішень. Розглянуто більш детально:

- види ідентифікації особистостей (парольна, біометрична та апаратна);
- біомеричний вид поділяється на статичні (фізіологічні) та динамічні (психологічні) характеритсики. Наприклад, статичні – відбитки пальців, сітчатка ока, ДНК тощо. До динамічних відносяться голос, почерк і т.д.;
- етапи ідентифікації людей;
- основні види біометрії, переваги і недоліки;
- технології ідентифікації.

Для вдалого рішення гібридизації було розглянуто існуючі види методів, а саме: багатосенсорні, мультимодальні, динамічна, комбінація біометрії та паролів, фузія.

Запропоноване рішення є досить універсальним у використанні, надає можливість використання в різних сферах.

Метою було гібридизувати методи ідентифікації особистостей з кращими результатами надійності, часу, безпеки, фінансових складових. У роботі запропоноване рішення мультимодальним методом, який поєднує в собі кілька зчитувачів біомтеричних характеристик з подальшою обробкою та ідентифікацією людини.

Новизна кваліфікаційної роботи полягає в створенні стійкого метода захисту доступу даних на основі гібридизації методу ідентифікації за біометричними характеристиками. Гібридизація є перспективним напрямком досліджень в області біометрії. Процес може привести до створення більш безпечних і надійних систем аутентифікації користувачів і ідентифікації осіб.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Wonki, L. Individual biometric identification using electrocardiographic waveform patterns [Текст] : довідник / L. Wonki, K. Seulgee, K. Daeeun. – 2018. – №4.

2. Gait recognition system: deep dive into this future tech [Електронний ресурс]. – Режим доступу : www/ URL: https://recfaces.com/articles/what-is-gait-recognition.

3. Gait recognition and analysis [Електронний ресурс]. – Режим доступу : www/ URL: https://www.exer.ai/posts/gait-recognition-using-deep-learning-to-collect-better-data.

4. Hanisch, S. Understanding person identification through gait [Текст] : довідник / S. Hanisch, E. Muschter, Li Shu-Chen, T. Strufe, A. Hatzipanayioti. – 2022.

5. An automated method for biometric handwritten signature authentication employing neural networks [Електронний ресурс]. – Режим доступу : www/ URL: https://www.mdpi.com/2079-9292/10/4/456.

6. How biometrics works [Електронний ресурс]. – Режим доступу : www/ URL: https://science.howstuffworks.com/biometrics.htm.

7. Romanov, V., Galelyuka, I., Klochan, P. Technologies for person authentication by using biometric characteristics [Текст] : довідник V. Romanov, I. Galelyuka, P. Klochan. – 2010. – № 9. – С. 54-61.

8. Plomondon, R., Lorette, G. Automatic signature verification and writer identification [Текст] : довідник R. Plomondon, G. Pattern Lorette – 1999. – № 2. – С.107-131.

9. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації / П. Бідюк, В. Бондарчук // Інститут прикладного системного аналізу. Національного технічного університету Київський політехнічний інститут. – 2009. – С. 137-147.

10. Царьов Р.Ю., Лемеха Т.М. Біометричні технології / Р.Ю. Царьов, Т.М. Лемеха // Одеська національна академія зв'язку ім. О.С. Попова. – 2016. – С. 19-69.

11. Захаров В.П., Рудешко В.І. Біометричні технології в XXI столітті та їх використання правоохоронними органами / В.П. Захаров, В.І. Рудешко // Львівський державний університет внутрішніх справ. – 2015. – С. 492.

12. Костомаха М.В. Комп'ютерна система біометричної аутентифікації особи за відбитком пальця / М.В. Костомаха // Терноільський національний технічний університет ім. Івана Пулюя. – 2021. – С. 83.

13. Tarasiants, A., Bondarenko, M. Method of creating a hybrid personal identification system based on biometric data / A. Tarasiants, M. Bondarenko // Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення». – Випуск 81. – 2023. – С. 81-82.

14. Налашутвання бібліотеки для зчитування [Електронний ресурс]. – Режим доступу : https://learn.microsoft.com/ru-ru/windows-hardware/test/hlk/testref/fingerprint-reader-testing-prerequisites

15. Jain, A., Hong, L., Pankanti, S. Biometric identification [Текст] : довідник / A. Jain, L. Hong, S. Pankanti. – 2000. – С. 50-72.