Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп’ютерної інженерії та управління
Кафедра Комп’ютерних інтелектуальних технологій та систем

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Інтелектуальна система доступу до приміщення по відбитку пальця

Виконав:
студент 2 курсу, групи КІТм-21-1
Свиридюк П.А.

Спеціальність 123 Комп’ютерна інженерія
Тип програми освітньо-професійна
Освітня програма Комп’ютерні інтелектуальні технології
Керівник доц. Сердюк Н.М

Допускається до захисту _____
(підпис)

Зав. кафедри _____ О.Г. Руденко
(підпис)

2022 р.

Харківський національний університет радіоелектроніки

Факультет	Комп’ютерної інженерії та управління
Кафедра	Комп’ютерних інтелектуальних технологій та систем
Рівень вищої освіти	другий (магістерський)
Спеціальність	123 Комп’ютерна інженерія
Тип програми	освітньо-професійна
Освітня програма	Комп’ютерні інтелектуальні технології

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«_____»_____2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Свиридюку Павлу Анатолійовичу

1. Тема роботи (проекту) Інтелектуальна система доступу до приміщення по відбитку пальця

затверджена наказом університету від "07" листопада 2022 р. № 1455_Ст

2. Термін подання студентом роботи до екзаменаційної комісії 19 грудня 2022 р.

3. Вихідні дані до роботи (проекту)

1) Середа розробки
2) Перелік питань, що потрібно опрацювати в роботі
3) Аналіз предметної області
4) Аналіз існуючих рішень
5) Аналіз та обрання методу або методів для обробки та аналізу
6) Програмна реалізація
7) Висновки

8. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.8включається до завдання за рішенням кафедри)

_____

_____

9. Консультанти розділів роботи (п.9 включається до завдання за наявністю консультантів згідно до наказу, зазначеному 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.	Видача та узгодження теми проекту	08.11.2022	виконано
2.	Аналіз предметної області	9.11.2022 -13.11.2022	виконано
3.	Аналіз існуючих рішень	14.11.2022	виконано
4.	Аналіз та обрання методу або методів для обробки та аналізу тексту	15.11.2022 - 17.11.2022	виконано
5.	Програмна реалізація Telegram-бота	18.11.2022 - 26.11.2022	виконано
6.	Відлагодження Telegram-бота	27.11.2022 - 29.11.2022	виконано
7.	Створення інструкції для користувача	30.11.2022	виконано
8.	Оформлення матеріалів атестаційної роботи	01.12.2022 - 4.12.2022	виконано
9.	Перевірка виконаного проекту керівником	5.12.2022	виконано
10.	Попередній захист	17.12.2022	виконано
11.	Захист проекту	20.12.2022	виконано

Дата видачі завдання 08 __листопада__2022 р.

Студент _____
(підпис)

Керівник роботи _____ _____доц. Сердюк Н.М._____
(підпис) (посада, ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 56 сторінок, 10 рисунків, 1 таблиць, 10 джерел.

Темою кваліфікаційної роботи є інтелектуальна система доступу до пріміщення по відбитку пальця.

Метою кваліфікаційної роботи є розробка багатофункціонального створення системи функціонал якоі дозволяє сканувати та роспізнавати особу по відбитку пальця.

Об'єктом дослідження цієї роботи є реалізація методів сканування відбитку, збереження зразку та аналіз відбитку при повторному скануванні з новим зразком відбитку пальця.

Відповідно до мети кваліфікаційної роботи виконано поставлені задачі. Виконано аналіз предметної області для виявлення актуальності розробки системи роспізнавання відбитку.

Проаналізовано існуючі рішення вже створених розробок, виявлено недоліки та переваги. Проаналізовано та обрано методи для обробки та аналізу відбитку з метою жосягнути максимальноі точності в роботі системи та уникнути небажаних системних помилок .

ІНФОРМАЦІЯ, АНАЛІЗ, ДОСЛІДЖЕННЯ, ВІДБИТОК ПАЛЬЦЯ, МАШИННЕ НАВЧАННЯ.

ABSTRACT

Explanatory note of the qualification work: 56 pages, 17 figures, 1 tables, 19 sources.

The subject of the qualification work is an intelligent fingerprint access system.
The method of qualification work is the development of a multifunctional creation of a functional system that allows you to scan and recognize a person by fingerprint.
The object of research of this work is the implementation of methods of fingerprint scanning, sample saving and fingerprint analysis when re-scanning with a new fingerprint sample.
the tasks set for the purpose of the qualification work have also been completed. An analysis of the subject area was performed for the relevance of the development of the fingerprint recognition system.
Existing solutions of already created developments were analyzed, shortcomings and advantages were revealed. The methods of print processing and analysis were analyzed and selected with the aim of achieving maximum accuracy in the work system and avoiding unwanted system errors.

INFORMATION, ANALYSIS, RESEARCH, FINGERPRINTING, MACHINE LEARNING.

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп’ютерної інженерії та управління
Кафедра Комп’ютерних інтелектуальних технологій та систем

АНОТАЦІЯ

КВАЛІФІКАЦІЙНОЇ РОБОТИ

рівень вищої освіти другий (магістерський)

Інтелектуальна система доступу до приміщення по відбитку пальця

(тема)

Виконав:
студент 2 курсу, групи КІТм-21-1
Свиридюк П.А.
(прізвище, ініціали)
Спеціальність 123 Комп’ютерна інженерія
Тип програми освітньо-професійна
Освітня програма Комп’ютерні інтелектуальні технології
Керівник доц. Сердюк Н.М

2022 р.

АНОТАЦІЯ

Свиридюк П.А. Інтелектуальна система доступу до приміщення по відбитку пальця – Магістерська кваліфікаційна робота.

Існує кілька форм біометричної ідентифікації, які використовуються для контролю доступу: відбиток пальця, геометрія руки, райдужна оболонка ока, розпізнавання голосу та розпізнавання обличчя.

Біометрична технологія просувається за її здатність значно підвищити рівень безпеки систем. Прихильники стверджують, що технологія усуває такі проблеми, як втрата, викрадення чи позика ідентифікаційних карток і забуті PIN-коди.

Усі біометричні зчитувачі працюють однаково, порівнюючи шаблон, що зберігається в пам’яті, зі сканом, отриманим під час процесу ідентифікації. Якщо існує достатньо висока ймовірність того, що шаблон у пам’яті сумісний із скануванням у реальному часі (сканування належить уповноваженій особі), ідентифікаційний номер цієї особи надсилається на панель керування.

Потім панель керування перевіряє рівень дозволу користувача та визначає, чи потрібно дозволити доступ. Зв'язок між зчитувачем і панеллю керування зазвичай передається за допомогою промислового стандартного інтерфейсу Wiegand. Єдиним винятком є інтелектуальний біометричний зчитувач, який не потребує жодних панелей і безпосередньо керує всією дверною фурнітурою.

Біометричні шаблони можуть зберігатися в пам'яті зчитувачів, обмежуючи кількість користувачів обсягом пам'яті зчитувачів (є моделі зчитувачів, що випускаються з ємністю до 50 000 шаблонів). Шаблони користувачів також можуть зберігатися в пам’яті смарт-карти, таким чином знімаючи всі обмеження на кількість користувачів системи (за допомогою цієї технології ідентифікація лише за допомогою пальця неможлива), або центральний серверний комп’ютер може виступати в якості хоста шаблону. У

системах, де використовується центральний сервер, відомий як «перевірка на основі сервера», зчитувачі спочатку зчитують біометричні дані користувача, а потім передають їх на головний комп’ютер для обробки. Серверні системи підтримують велику кількість користувачів, але залежать від надійності центрального сервера, а також ліній зв’язку.

У режимі 1-до-1 користувач повинен спочатку або пред'явити посвідчення особи, або ввести PIN-код. Потім зчитувач шукає шаблон відповідного користувача в базі даних і порівнює його з реальним скануванням. Метод 1-до-1 вважається більш безпечним і, як правило, швидшим, оскільки читачеві потрібно виконати лише одне порівняння. Більшість біометричних зчитувачів 1-до-1 є зчитувачами з «подвійною технологією»: вони або мають вбудований зчитувач безконтактних карт, смарт-карт або клавіатури, або мають вхід для підключення зовнішнього зчитувача карток.

У режимі «1-до-багатьох» користувач надає біометричні дані, такі як відбиток пальця або сканування сітківки ока, а потім зчитувач порівнює живе сканування з усіма шаблонами, збереженими в пам’яті. Більшість кінцевих користувачів віддають перевагу цьому методу, оскільки він усуває необхідність носити при собі ідентифікаційні картки чи використовувати PIN-коди. З іншого боку, цей метод є повільнішим, тому що читачеві може знадобитися виконати тисячі операцій порівняння, поки він не знайде збіг. Важливою технічною характеристикою зчитувача 1-до-багатьох є кількість порівнянь, які можна виконати за одну секунду, що вважається максимальним часом, протягом якого користувачі можуть чекати біля дверей, не помічаючи затримки. Наразі більшість зчитувачів 1-до-багатьох здатні виконувати 2000–3000 операцій зіставлення за секунду.

У ході виконання роботи було зроблено ряд висновків на основі практичних результатів, отриманих від впроваджених систем, і наступні є найважливішими з них:

1) Отриманно зображення відбитків пальців декількох осіб із нашої реальності різного віку та обертання зображення відбитків пальців, наскільки це можливо, означає, що кінцеві результати є більш реальними та

застосовними.

2) Включення покращення зображення в систему ідентифікації відбитків пальців покращує якість вхідного зображення відбитків пальців, зменшує виділення хибних векторів ознак і мінімізує помилки зіставлення.

3) Алгоритм вилучення основних точок і потенційних основних точок є хорошим алгоритмом і підходить як основа для алгоритму вилучення ознак.

4) Алгоритм виділення ознак на основі алгоритму Filterbank_based створює хороший вектор ознак у порівнянні між відбитками пальців, що відрізняються від однієї людини до іншої.

5) Нейронні мережі KNN забезпечують відповідний результат відповідності, а 70% порогове значення методу забезпечує належні та хороші результати для зображень FP (90 осіб і 8 зразків для кожного), які належать до бази даних, що становить 93,9683% коефіцієнт розпізнавання.

ІНФОРМАЦІЯ, АНАЛІЗ, ДОСЛІДЖЕННЯ, ВІДБИТОК ПАЛЬЦЯ, МАШИННЕ НАВЧАННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

KNN – K Nearest Neightbour

BKNN – Boolean k-nearest neighbor

FP – Fingerprint

FAR – False Acceptance Rate

FPGA – Field Programming Gate Array

ID – Identifier

ВСТУП

Відбиток пальця – це відбиток, який залишають тертя пальця людини. Відновлення часткових відбитків пальців на місці злочину є важливим методом криміналістики. Волога та жир на пальці призводять до утворення відбитків пальців на таких поверхнях, як скло чи метал. Навмисні відбитки цілих відбитків пальців можна отримати за допомогою чорнила або інших речовин, перенесених з вершин тертя на шкірі на гладку поверхню, наприклад папір. Записи відбитків пальців зазвичай містять відбитки подушечок на останньому суглобі пальців і великих пальців, хоча картки відбитків пальців також зазвичай записують частини нижніх суглобів пальців.

Відбитки пальців - це відбитки, залишені на поверхнях від тертя на пальці людини. Зіставлення двох відбитків пальців є одним з найпоширеніших і найнадійніших біометричних методів. Зіставлення відбитків пальців враховує лише очевидні особливості відбитків пальців.[1]

Склад відбитків пальців складається з води (95%-99%), а також органічних і неорганічних компонентів. Органічний компонент складається з амінокислот, білків, глюкози, лактази, сечовини, пірувату, жирних кислот і стеролів. Також присутні неорганічні іони, такі як хлорид, натрій, калій і залізо. Інші забруднювачі, такі як олії, які містяться в косметиці, ліках та їх метаболіти та залишки їжі, можуть бути знайдені в залишках відбитків пальців.[2]

Відбитки пальців людини деталізовані, майже унікальні, їх важко змінити та зберігаються протягом життя людини, що робить їх придатними як довготривалі маркери людської особистості. Вони можуть використовуватися поліцією чи іншими органами влади для ідентифікації осіб, які бажають приховати свою особу, або для ідентифікації людей, які є недієздатними чи померлими і тому не можуть ідентифікувати себе, як, наприклад, після стихійного лиха.

Їх використання як доказів було оскаржено науковцями, суддями та ЗМІ. Немає єдиних стандартів для методів підрахунку балів, і вчені стверджують, що

частота помилок у зіставленні відбитків пальців не була належним чином вивчена і що докази відбитків пальців не мають надійної статистичної основи. Було проведено дослідження щодо того, чи можуть експерти об’єктивно зосередитися на інформації про особливості у відбитках пальців, не вводячись в оману сторонньою інформацією, такою як контекст.

Відповідно до мети кваліфікаційної роботи необхідно виконати поставлені задачі, а саме:

– виконати аналіз предметної області для виявлення актуальності розробки;

– проаналізувати існуючі рішення для виявлення вже створених розробок, їх недоліків та переваг;

– проаналізувати та обрати метод або методи для обробки та аналізу відбитків пальців;

– реалізувати систему яка буде спроміжна на сканування та роспізнавання відбитків пальців;

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

З появою шовку та паперу в Китаї сторони юридичного договору відображали на документі відбитки своїх рук. Десь перед 851 р. н. е. арабський купець у Китаї Абу Зайд Хасан був свідком того, як китайські торговці використовували відбитки пальців для перевірки автентичності позик.

Хоча стародавні народи, ймовірно, не усвідомлювали, що відбитки пальців можуть однозначно ідентифікувати людей, згадки часів вавилонського царя Хаммурапі (правив у 1792–1750 рр. до н.е.) вказують на те, що правоохоронці знімали відбитки пальців людей, яких було заарештовано. Під час династії Цінь у Китаї записи показали, що чиновники знімали відбитки рук і ніг, а також відбитки пальців як докази на місці злочину. У 650 році китайський історик Кіа Кунг-Єн зауважив, що відбитки пальців можна використовувати як засіб ідентифікації. У своїй «Джамі аль-Таваріх» («Всесвітня історія») іранський лікар Рашид-ад-Дін Хамадані (1247–1318) згадує про китайську практику ідентифікації людей за відбитками пальців, коментуючи: «Досвід показує, що немає двох людей із абсолютно однаковими пальцями.

Рисунок 1.1 - Відбитки пальців замість підписів на індійському юридичному документі 1952 року

З кінця 16 століття і далі європейські вчені намагалися включити відбитки пальців у наукові дослідження. Але правдоподібні висновки можна було зробити лише з середини XVII століття. У 1686 році професор анатомії Болонського університету Марчелло Мальпігі виявив виступи, спіралі та петлі у відбитках пальців, залишених на поверхнях. У 1788 році німецький анатом Йоганн Крістоф Андреас Майєр був першим європейцем, який дійшов висновку, що відбитки пальців є унікальними для кожної людини. У 1880 році Генрі Фолдс на основі своїх досліджень припустив, що відбитки пальців є унікальними для людини.

Ідентифікація особи в цифровому середовищі може бути виконана трьома основними способами, тобто за допомогою «чогось, що відомо» (наприклад, пароль, PIN-код тощо), «чогось носимого» (наприклад, ідентифікаційні картки, ключі тощо) або «чогось наявного» (наприклад, відбитки пальців, обличчя, ірис тощо). Встановлено, що системи безпеки та розпізнавання, засновані на сурогатних представленнях, наприклад паролі та ідентифікаційні картки, мають фундаментальний недолік, наприклад, пароль можна забути або вгадати, ідентифікаційну картку можна легко втратити або загубити, і всі вони можуть бути досить легко підроблені.

У 1823 році Ян Євангеліста Пуркіне ідентифікував дев'ять зразків відбитків пальців. Дев'ять візерунків включають наметову арку, петлю та завиток, які в сучасній криміналістиці вважаються деталями хребта. У 1840 році, після вбивства лорда Вільяма Рассела, провінційний лікар Роберт Блейк Овертон написав до Скотленд-Ярду пропозицію перевірити відбитки пальців.

У 1853 році німецький анатом Георг фон Мейснер (1829–1905) вивчав гребені тертя, а в 1858 році сер Вільям Джеймс Гершель започаткував дактилоскопію в Індії. У 1877 році він вперше запровадив використання відбитків пальців на контрактах і документах, щоб запобігти відмові від підписів у Хуглі поблизу Калькутти, і він зареєстрував відбитки пальців державних пенсіонерів, щоб запобігти збору грошей родичами після смерті пенсіонера.

Рисунок 1.2 - Дев'ять шаблонів відбитків пальців, визначених Яном Євангелістою Пуркіне

У 1880 році Генрі Фолдс, шотландський хірург у токійській лікарні, опублікував свою першу статтю про корисність відбитків пальців для ідентифікації та запропонував метод їх запису друкарською фарбою. Повернувшись до Великої Британії в 1886 році, він запропонував концепцію столичній поліції в Лондоні, але в той час її відхилили. Аж до початку 1890-х років поліцейські сили в Сполучених Штатах і на європейському континенті не могли достовірно ідентифікувати злочинців для відстеження їх судимості.

Френсіс Гальтон опублікував детальну статистичну модель аналізу та ідентифікації відбитків пальців у своїй книзі «Відбитки пальців» 1892 року. Він підрахував, що ймовірність «помилкового спрацьовування» (дві різні особи мають однакові відбитки пальців) була приблизно 1 до 64 мільярдів. У 1892 році Хуан Вучетич, аргентинський старший офіцер поліції, створив перший метод запису відбитків пальців осіб у файлі.

Того ж року Франсіску Рохас знайшли в будинку з пораненнями на шиї, а двох її синів знайшли мертвими з перерізаними горлами. Рохас звинуватив сусіда, але, незважаючи на жорстокий допит, той не зізнався у злочинах. Інспектор Альварес, колега Вуцетіча, виїхав на місце події та знайшов закривавлений слід від великого пальця на дверях. Коли його порівняли з

відбитками Рохас, виявилося, що він ідентичний великому пальцю її правої руки. Потім вона зізналася у вбивстві своїх синів. Це була перша відома справа про вбивство, розкрита за допомогою аналізу відбитків пальців.

У 1930-х роках кримінальні слідчі в Сполучених Штатах вперше виявили наявність прихованих відбитків пальців на поверхнях тканин, особливо на внутрішніх сторонах рукавичок, викинутих злочинцями.

З кінця дев'ятнадцятого століття методи ідентифікації за відбитками пальців використовувалися поліцейськими службами в усьому світі для ідентифікації підозрюваних злочинців, а також жертв злочинів.[3] Основа традиційної техніки зняття відбитків пальців проста. Шкіра на долонній поверхні кистей і стоп утворює валики, так звані папілярні валики, унікальні для кожної людини і не змінювані з часом. Навіть однояйцеві близнюки (які мають спільну ДНК) не мають ідентичних відбитків пальців. Найкращий спосіб відобразити приховані відбитки пальців, щоб їх можна було сфотографувати, може бути складним і залежати, наприклад, від типу поверхні, на якій вони були залишені. Як правило, необхідно використовувати «проявник», як правило, порошок або хімічний реагент, щоб створити високий ступінь візуального контрасту між візерунками гребнів і поверхнею, на яку було нанесено відбиток пальця.

Рисунок 1.3 - Використання дрібної пудри та пензлика для виявлення прихованих відбитків пальців

Ефективність проявників залежить від присутності органічних матеріалів або неорганічних солей, хоча вода, що осідає, також може відігравати ключову роль. Відбитки пальців, як правило, утворюються з водянистих виділень еккринних залоз пальців і долонь із додатковим матеріалом із сальних залоз, головним чином із чола. Останнє забруднення є наслідком звичайної людської поведінки – торкання обличчя та волосся. Отримані приховані відбитки зазвичай складаються із значної частки води з невеликими слідами амінокислот і хлоридів, змішаних з жирним сальним компонентом, який містить ряд жирних кислот і тригліцеридів. Виявлення невеликої частки реакційноздатних органічних речовин, таких як сечовина та амінокислоти, непросте.

Відбитки пальців на місці злочину можна виявити за допомогою простих порошків або хімічних речовин, застосованих на місці. Більш складні методи, як правило, із застосуванням хімікатів, можуть бути застосовані в спеціалізованих лабораторіях до відповідних предметів, вилучених з місця злочину. З удосконаленням цих більш складних методів деякі з більш передових служб розслідування місця злочину з усього світу станом на 2010 рік повідомляли, що 50% або більше відбитків пальців, знайдених на місці злочину, було ідентифіковано в результаті лабораторних досліджень. засновані техніки.

У Калькутті Бюро відбитків пальців було створено в 1897 році після того, як Рада генерал-губернатора схвалила звіт комітету про те, що відбитки пальців слід використовувати для класифікації судимостей. Співробітникам бюро Азізулу Хаку та Хему Чандрі Бозу приписують першочергову розробку системи класифікації відбитків пальців, яку врешті назвали на честь їх керівника, сера Едварда Річарда Генрі.

Неурядова організація Privacy International у 2002 році зробила попереджувальне оголошення про те, що школи беруть відбитки пальців у десятків тисяч британських школярів, часто без відома чи згоди їхніх батьків. Того ж року компанія-постачальник Micro Librarian Systems, яка використовує технологію, подібну до тієї, що використовується в американських в’язницях і

німецьких військових, підрахувала, що 350 шкіл по всій Британії використовують такі системи для заміни бібліотечних карток.

До 2007 року, за оцінками, 3500 шкіл використовували такі системи. Відповідно до Закону Сполученого Королівства про захист даних, школи у Великій Британії не повинні запитувати згоду батьків, щоб дозволити такі дії. Батьки, які виступають проти дактилоскопії, можуть подавати лише індивідуальні скарги на школи.

У відповідь на скаргу, яку вони продовжують розглядати, у 2010 році Європейська комісія висловила «значне занепокоєння» щодо пропорційності та необхідності такої практики та відсутності судового захисту, вказавши, що така практика може порушити директиву Європейського Союзу щодо захисту даних.

У березні 2007 року уряд Великої Британії розглядав можливість зняття відбитків пальців у всіх дітей віком від 11 до 15 років і додавання відбитків до державної бази даних у рамках нової схеми паспортів та ідентифікаційних карток і заборони опозиції з міркувань конфіденційності.

Усі взяті відбитки пальців будуть перевірятися з відбитками 900 000 нерозкритих злочинів. Тіньовий міністр внутрішніх справ Девід Девіс назвав план "зловісним". Речник ліберал-демократів у внутрішніх справах Нік Клегг розкритикував «рішучість побудувати державу спостереження за спинами британського народу».

Міністр молодшої освіти Великої Британії лорд Адоніс захистив використання відбитків пальців у школах для відстеження відвідування школи, а також доступу до шкільних обідів і бібліотек, і запевнив Палату лордів, що відбитки пальців дітей були взяті за згодою батьків і будуть бути знищені, як тільки діти залишать школу. Пропозиція Early Day Motion, яка закликала уряд Великобританії провести повні та відкриті консультації із зацікавленими сторонами щодо використання біометрії в школах, отримала підтримку 85 членів парламенту. Після створення у Сполученому Королівстві консервативно-ліберально-демократичного коаліційного уряду в травні 2010 року систему ідентифікаційних карток у Великобританії було скасовано.

Серйозне занепокоєння щодо наслідків для безпеки використання звичайних біометричних шаблонів у школах було піднято кількома провідними експертами з IT-безпеки, один з яких висловив думку, що «абсолютно передчасно починати використовувати «звичайну біометрію» в школах. Постачальники біометричних систем стверджують, що їхня продукція приносить школам такі переваги, як покращення навичок читання, скорочення часу очікування в обідніх чергах і збільшення доходів. Вони не посилаються на незалежні дослідження на підтримку цієї точки зору. Один фахівець у галузі освіти написав у 2007 році: «Мені не вдалося знайти жодного опублікованого дослідження, яке б свідчило про те, що використання біометрії в школах сприяє здоровому харчуванню чи покращує навички читання серед дітей... Для таких тверджень немає абсолютно жодних доказів.

Дуже рідкісний медичний стан, адерматогліфія, характеризується відсутністю відбитків пальців. Постраждалі особи мають абсолютно гладкі кінчики пальців, долоні, пальці ніг і підошви, але жодних інших медичних ознак або симптомів немає. Дослідження 2011 року показало, що адерматогліфія спричинена неправильною експресією білка SMARCAD1. Дослідники, які його описують, назвали цей стан хворобою затримки імміграції, оскільки вроджена відсутність відбитків пальців викликає затримки, коли постраждалі люди намагаються підтвердити свою особу під час подорожі. Станом на 2011 рік було описано лише п’ять сімей з таким захворюванням.

У людей із синдромом Нагелі–Франческетті–Ядассона та сітчастою пігментною дерматопатією, які є формами ектодермальної дисплазії, також немає відбитків пальців. Обидва ці рідкісні генетичні синдроми викликають інші ознаки та симптоми, такі як тонке, ламке волосся.

У злочинця Елвіна Карпіса хірургічним шляхом видалили відбитки пальців у 1933 році

Протираковий препарат капецитабін може спричинити втрату відбитків пальців. Набряк пальців, наприклад, спричинений укусами бджіл, у деяких випадках спричиняє тимчасове зникнення відбитків пальців, хоча вони повертаються, коли набряк спадає.

Оскільки еластичність шкіри з віком знижується, у багатьох людей похилого віку є відбитки пальців, які важко зняти. Хребти стають товщі; висота між верхньою частиною хребта та нижньою частиною борозни стає вузькою, тому помітність стає меншою.

Відбитки пальців можна стерти назавжди, і цим потенційно можуть скористатися злочинці, щоб зменшити свої шанси на засудження. Стирання можна досягти різними способами, включаючи простий опік кінчиків пальців, використання кислот і передових методів, таких як пластична хірургія. Джон Діллінджер обпік собі пальці кислотою, але відбитки, зроблені під час попереднього арешту та після смерті, усе ще виявляли майже повний зв’язок один з одним.

Біометричні системи розпізнавання широко використовуються в ряді поточних і потенційних застосувань, починаючи від національної безпеки, правоохоронних органів, ідентифікації людей, зокрема для контролю доступу до будівель, ідентифікація підозрюваних поліцією, водійські права та багато інших сфер. Таким чином, сучасні тенденції розвитку інноваційних систем безпеки, зокрема щодо ідентифікації та верифікації особи, приділяють значну увагу біометричним рішенням з тієї причини, що в біометричних системах ідентифікації ключем є користувач. Біометричні технології можна визначити як «автоматизовані методи перевірки або розпізнавання особистості людини на основі фізіологічних та/або поведінкових характеристик». На рис. 1.4 наведені біометричні ознаки, які зазвичай використовуються, включаючи відбитки пальців, обличчя, райдужну оболонку ока (ірис), відбиток долоні, підпис і голос.

Процес машинного навчання починається з введення навчальних даних в обраний алгоритм. Нові вхідні дані подаються в алгоритм машинного навчання для перевірки правильності роботи алгоритму. Прогноз і результати потім перевіряються один проти одного.

Рисунок 1.4 - Приклад деяких часто використовуваних біометричних характеристик

Зіставлення вен, також зване судинною технологією, є технікою біометричної ідентифікації за допомогою аналізу візерунків кровоносних судин, видимих на поверхні шкіри. Незважаючи на те, що цей метод ідентифікації використовується Федеральним бюро розслідувань і Центральним розвідувальним управлінням, він все ще розробляється і ще не був повсюдно прийнятий кримінальними лабораторіями, оскільки він не вважається таким надійним, як більш усталені методи, такі як зняття відбитків пальців. Однак його можна використовувати в поєднанні з наявними судово-медичними даними на підтримку висновку.

У той час як інші типи біометричних сканерів ширше використовуються в системах безпеки, судинні сканери стають все більш популярними. Сканери відбитків пальців використовуються частіше, але вони, як правило, не надають достатньо точок даних для критичних рішень перевірки.

Оскільки сканери відбитків пальців вимагають прямого контакту пальця зі сканером, суха або потерта шкіра може заважати надійності системи. Шкірні захворювання, такі як псоріаз, також можуть обмежувати точність сканера, не кажучи вже про те, що прямий контакт зі сканером може призвести до

необхідності частішого очищення та підвищеного ризику пошкодження обладнання. З іншого боку, сканери судин не потребують контакту зі сканером, і оскільки інформація, яку вони зчитують, знаходиться всередині тіла, захворювання шкіри не впливають на точність зчитування.

Судинні сканери також працюють дуже швидко, скануючи менш ніж за секунду. Під час сканування вони фіксують унікальний візерунок вен, які розгалужуються на руці. Сканер сітківки більш надійний, ніж сканер судин, але використовується менш широко через його інтрузивний характер. Людям, як правило, незручно піддавати очі незнайомому джерелу світла, а сканери сітківки ока важче встановити, ніж обладнання для сканування судин, оскільки необхідно враховувати різницю у висоті й куті обличчя відносно пристрою.[4]

Джо Райс, інженер із систем автоматизованого керування на фабриці Kodak у Аннеслі, винайшов розпізнавання вен на початку 1980-х років у відповідь на викрадення його банківських карток та посвідчення особи. Він розробив те, що по суті було зчитувачем штрих-кодів для використання на тілі людини, і передав права британській NRDC (Національна корпорація з розвитку досліджень). (Тетчер приватизувала NRDC у BTG) незначно просунулися в технології ліцензування шаблонів жилок. Світ був прив’язаний до відбитків пальців і візерунків райдужної оболонки, і уряди (основні покупці біометричних рішень) хотіли біометричних даних відкритого перегляду для цілей спостереження, а не прихованого персонального біометричного рішення.

Наприкінці 1990-х BTG заявили, що вони видаляють візерунки вен через відсутність комерційного інтересу. Райс був незадоволений рішенням BTG і впровадженням ними технології візерунка вен, тому він виступив на Біометричному саміті у Вашингтоні, округ Колумбія, про те, як він розробить розпізнавання візерунка вен.[8] Цій точці зору заперечив наступний доповідач з IBG (Міжнародної біометричної групи, що базується в США), який сказав, що у візерунках вен недостатньо інформації, щоб використовувати їх як життєздатні біометричні дані.

У 2002 році Hitachi і Fujitsu випустили біометричні продукти для вени, і вени виявилися одними з найбільш послідовних, дискримінаційних і точних біометричних ознак. У середині 2000-х Райс отримала запрошення від Матіаса Ваноні стати партнером швейцарської компанії Biowatch SA для розробки та комерціалізації біогодинників.

Технологія розпізнавання судинних/венозних структур (VPR) була комерційно розроблена Hitachi з 1997 року, за якою інфрачервоне світло, поглинене гемоглобіном у кровоносних судинах суб'єкта, записується (як темні візерунки) камерою CCD за прозорою поверхнею. Шаблони даних обробляються, стискаються та оцифровуються для майбутньої біометричної автентифікації суб'єкта. Експерт з комп'ютерної безпеки Брюс Шнайер заявив, що ключовою перевагою візерунків вен для біометричної ідентифікації є відсутність відомого методу підробки придатного для використання «манекена», як це можливо з відбитками пальців.

Візерунки кровоносних судин унікальні для кожної людини, як і інші біометричні дані, такі як розпізнавання відбитків пальців або візерунки райдужної оболонки ока. На відміну від деяких біометричних систем, візерунки кровоносних судин майже неможливо підробити, оскільки вони розташовані під поверхнею шкіри. Біометричні системи, засновані на відбитках пальців, можна обдурити за допомогою манекена пальця, оснащеного скопійованим відбитком пальця; Системи, засновані на характеристиках голосу та обличчя, можна обдурити записами та зображеннями з високою роздільною здатністю. Систему ідентифікації вен на пальці набагато важче обдурити, оскільки вона може ідентифікувати лише палець живої людини.

Розпізнавання вен пальців ґрунтується на зображеннях вен людських пальців під поверхнею шкіри. В даний час технологія використовується або розробляється для широкого спектру додатків, включаючи автентифікацію кредитних карток, безпеку автомобіля, відстеження робочого часу та відвідуваності співробітників, автентифікацію комп'ютера та мережі, безпеку кінцевої точки та банкомати.

Щоб отримати шаблон для запису бази даних, особа вставляє палець у термінал атестера, що містить світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне світлодіодне підсвічування ближнього інфрачервоного діапазону та камеру монохромного пристрою із зарядовим зв'язком (CCD). Гемоглобін у крові поглинає світлодіодне світло ближнього інфрачервоного діапазону, через що система вен виглядає як темний малюнок ліній. Камера записує зображення, а необроблені дані оцифровуються, сертифікуються та надсилаються до бази даних зареєстрованих зображень. З метою аутентифікації палець сканується, як і раніше, і дані надсилаються в базу даних зареєстрованих зображень для порівняння. Процес аутентифікації займає менше двох секунд.

Пристрої для сканування пальців були розгорнуті для використання в японських фінансових установах, кіосках і турнікетах. Mantra Softech продала в Індії пристрій, який сканує візерунки вен на долонях для реєстрації відвідуваності. Компанія Fujitsu розробила версію, яка не потребує прямого фізичного контакту зі сканером вен для покращення гігієни під час використання електронних пристроїв у торгових точках.

У 2020 році Ламберт Сонна Момо розробив нове покоління сканера VenoScannerF, який сканує вени пальців у кількох режимах перегляду та витягує ключ, зашифрований від кінця до кінця випадковим кодом, який постійно змінюється. Він розробляє нову версію з плаваючою рукою, яка буде доступна на ринку в 2022 році.[5]

Біометрична система, незалежно від алгоритмів, складається з чотирьох основних модулів: модуль датчика, модуль виділення ознак, модуль відповідності та модуль прийняття рішень.

Модуль датчика (сенсорний) фіксує біометричні дані користувача. Наприклад, датчик відбитків пальців, який знімає відбитки пальців користувача.

У модулі вилучення ознак отримані дані обробляються для вилучення наборів функцій. Наприклад, положення та орієнтація деталей на зображенні відбитка пальця обчислюватимуться в модулі вилучення функцій системи відбитків пальців.

Модуль відповідності порівнює набори функцій із системною базою даних, генеруючи оцінку відповідності. Наприклад, кількість відповідних деталей між запитом і шаблоном можна обчислити як оцінку відповідності.

Модуль прийняття рішень - де заявлена особа користувача або збігається, або не збігається, якщо оцінка збігу перевищує порогове значення системи, а якщо ні, оголошує невідповідність.

Біометрична система автентифікації - це, по суті, система розпізнавання образів, яка розпізнає особу шляхом визначення автентичності біометричних ознак, Біометрична система працює в три основні етапи.

Реєстрація: система збирає біометричні дані від користувача, а функції, витягнуті з даних, зберігаються як біометричний шаблон.

Перевірка: система ідентифікує особу людини шляхом порівняння отриманих біометричних даних з попередньо зареєстрованим біометричним довідковим шаблоном, попередньо збереженим у системі. Він проводить однозначне порівняння, щоб підтвердити, чи правдиве твердження про особу.

Ідентифікація: система розпізнає особу шляхом пошуку відповідності у всій базі даних шаблонів реєстрації. Тут проводиться порівняння один-до-багатьох, щоб визначити, чи присутня особа в базі даних, і якщо так, повертає ідентифікатор посилання на реєстрацію.

Біометрична система вразлива до різних типів атак, які можуть поставити під загрозу безпеку системи. Різні фактори, які впливають на безпеку системи, зазвичай належать до однієї з чотирьох категорій: внутрішні збої, адміністративні атаки, незахищена інфраструктура та доступ до біометричних даних.

Попередня обробка покращує якість зображення шляхом фільтрації та видалення сторонніх шумів. Алгоритм на основі дрібниць ефективний лише з 8-бітними зображеннями відбитків пальців у градаціях сірого. Однією з причин цього є те, що 8-бітне сіре зображення відбитка пальця є фундаментальною основою для перетворення зображення в 1-бітне зображення зі значенням 1 для гребнів і значенням 0 для борозен. [6]

Цей процес дозволяє покращити розпізнавання країв, тому відбиток пальця розкривається з високим контрастом, із виступами, виділеними чорним, а борознами – білим. Для подальшої оптимізації якості вхідного зображення потрібні ще два кроки: вилучення дрібниць і видалення помилкових дрібниць. Вилучення дрібниць виконується шляхом застосування алгоритму потоншення гребнів, який видаляє зайві пікселі гребнів.

У результаті стоншені гребені зображення відбитка пальця позначаються унікальним ідентифікатором для полегшення проведення подальших операцій. Після вилучення дрібниць проводиться видалення помилкових міток. Недостатня кількість чорнила та перехресний зв’язок між ребрами можуть спричинити помилкові дрібниці, які призведуть до неточності в процесі розпізнавання відбитків пальців.

Алгоритми на основі шаблонів порівнюють базові шаблони відбитків пальців (дуга, виток і петля) між попередньо збереженим шаблоном і потенційним відбитком. Для цього потрібно, щоб зображення можна було вирівняти в однаковій орієнтації. Для цього алгоритм знаходить центральну точку на зображенні відбитка пальця та центрується на ній. В алгоритмі на основі шаблону шаблон містить тип, розмір і орієнтацію візерунків у вирівняному зображенні відбитка пальця. Зображення відбитка пальця кандидата графічно порівнюється з шаблоном, щоб визначити ступінь їх збігу.

Внутрішні збої - це порушення безпеки через неправильне рішення, прийняте біометричною системою. Датчик може не отримати біометричні дані користувача через обмеження технології вимірювання або умови

навколишнього середовища. Варіації в умовах візуалізації фіксують біометричні дані, і, отже, витягнуті функції зазвичай демонструють значну схожість між користувачами та внутрішньокористувацькими варіаціями. Наприклад, зображення обличчя двох однояйцевих близнюків дуже схожі одне на одного, і це може призвести до неправильного рішення під час перевірки ідентичності одного з близнюків. Частота помилок, з якою система біометричної перевірки невірно збігається з двома непов'язаними біометричними шаблонами, називається коефіцієнтом помилкових прийомів (КПП). І навпаки, він також може не відповідати двом біометричним шаблонам, отриманим з однієї біометрії, через значні внутрішньокористувацькі варіації системи - частка помилкових відхилень (ЧПВ).

Адміністративні атаки - це відноситься до всіх вразливостей через неправильне адміністрування біометричної системи. Може статися зловживання функціями системи зловмисником шляхом змови з системним адміністратором, або примушення його дозволити особі зареєструватися, бути прийнятою як справжній користувач.

Незахищена інфраструктура - тут зловмисник може маніпулювати біометричною інфраструктурою в апаратному забезпеченні, програмному забезпеченні та каналах зв'язку між різними модулями.

Доступ до біометричних характеристик, зловмисник таємно захоплює біометричні дані законного користувача та використовує їх для створення фізичних артефактів. Отже, якщо система не здатна відрізнити живу біометричну інформацію від штучної підробки, зловмисник може обійти систему, представивши підроблені ознаки.

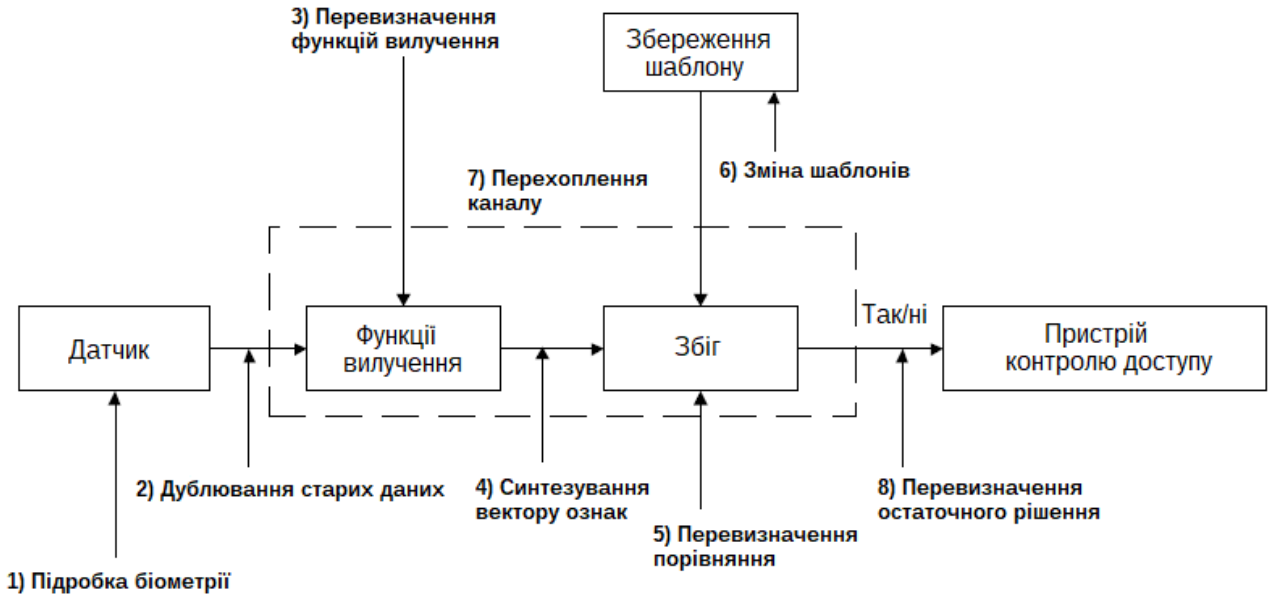

Рисунок 1.5 - Вразливості в системі біометричної ідентифікації

Оскільки такі біометричні системи схильні до вразливості в різних точках системи, ці атаки мають на меті або обійти захист, який забезпечує система, або змінити нормальне функціонування системи шляхом: на датчику може бути представлена підроблена біометрична ознака, наприклад штучний відбиток пальця. Незаконно перехоплені дані можуть бути повторно передані в систему. Екстрактор функцій може бути замінений троянською програмою, яка створює заздалегідь визначені набори функцій. Законні набори функцій можуть бути замінені синтетичними наборами функцій. Збіг може бути замінений троянською програмою, яка завжди виводить високі бали, тим самим кидаючи виклик безпеці системи.

2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

До комп’ютеризації у великих сховищах відбитків пальців використовувалися ручні системи файлів. Система класифікації відбитків пальців групує відбитки пальців відповідно до їхніх характеристик і, таким чином, допомагає зіставити відбиток пальця з великою базою даних відбитків пальців. Таким чином, відбиток запиту, який потрібно зіставити, можна порівняти з підмножиною відбитків в існуючій базі даних. Ранні системи класифікації ґрунтувалися на загальних візерунках хребта, включаючи наявність або відсутність круглих візерунків кількох або всіх пальців. Це дозволило зберігати та відновлювати паперові записи у великих колекціях лише на основі візерунків тертя. Найпопулярніші системи використовували клас шаблону кожного пальця для формування числового ключа для допомоги у пошуку в системі файлів. Системи класифікації відбитків пальців включали систему Рошера, систему Хуана Вуцетіча та систему класифікації Генрі. Система Рошера була розроблена в Німеччині та впроваджена в Німеччині та Японії. Система Вуцетіча була розроблена в Аргентині та впроваджена по всій Південній Америці. Система класифікації Генрі була розроблена в Індії та впроваджена в більшості англомовних країн.[7]

У класифікаційній системі Генрі є три основні візерунки відбитків пальців: петля, обертання та арка, які становлять 60–65 відсотків, 30–35 відсотків та 5 відсотків усіх відбитків пальців відповідно. складні системи класифікації, які ще більше розбивають візерунки на прості арки або наметові арки і на петлі, які можуть бути радіальними або ліктьовими, залежно від сторони руки, на яку спрямований хвіст.

Ліктьові петлі починаються на стороні мізинця пальця, стороні ближче до ліктьової кістки, нижньої кістки руки. Радіальні петлі починаються з боку великого пальця, сторона ближче до променевої кістки. Завитки також можуть класифікуватися за підгрупами, включаючи звичайні завитки, випадкові

завитки, завитки з подвійною петлею, завитки з павиним оком, композитні завитки та завитки з центральною петлею.

Рисунок 2.1 - Зображення відбитка пальця з позначеними на ньому основними точками

Консенсус у науковому співтоваристві припускає, що дерматогліфічні візерунки на кінчиках пальців є спадковими. Було показано, що моделі відбитків пальців монозиготних близнюків дуже схожі, тоді як дизиготні близнюки мають значно меншу схожість. Значна спадковість була виявлена для 12 дерматогліфічних характеристик. Сучасні моделі успадкування дерматогліфічних ознак припускають менделівську передачу з додатковими ефектами від адитивних або домінантних основних генів.

Тоді як гени визначають загальні характеристики візерунків і їх тип, наявність факторів навколишнього середовища призводить до незначної диференціації кожного відбитка пальця. Однак відносний вплив генетичних впливів і впливу навколишнього середовища на візерунки відбитків пальців загалом незрозумілий. Одне дослідження показало, що приблизно 5% загальної мінливості пов’язано з невеликими впливами навколишнього середовища, хоча це було виконано лише з використанням загальної кількості хребтів як метрики.

Було запропоновано кілька моделей механізмів формування пальцевих валиків, які призводять до великої різноманітності відбитків пальців. Одна модель припускає, що нестабільність викривлення в базальному клітинному шарі епідермісу плода відповідає за розвиток епідермальних валиків. Крім того, кровоносні судини та нерви також можуть відігравати важливу роль у формуванні конфігурації хребта.

Інша модель вказує на те, що зміни в амніотичній рідині, що оточує кожен розвивається палець у матці, спричиняють зростання відповідних клітин на кожному відбитку пальця в різних мікросередовищах. Для конкретної людини ці різні фактори впливають на кожен палець по-різному, запобігаючи тому, що два відбитки пальців не будуть ідентичними, але зберігають схожі візерунки.

Важливо зазначити, що визначення успадкування відбитків пальців ускладнюється великою різноманітністю фенотипів. Класифікація конкретного візерунка часто є суб’єктивною (відсутність консенсусу щодо найбільш прийнятної характеристики для кількісного вимірювання), що ускладнює аналіз дерматогліфічних візерунків.

Для різних шаблонів відбитків пальців було запропоновано та помічено декілька способів успадкування. Вважається, що загальна кількість відбитків пальців, широко використовуваний показник розміру візерунка відбитків пальців, має полігенний спосіб успадкування і на нього впливають численні адитивні гени. Однак ця гіпотеза була оскаржена іншими дослідженнями, які вказують на те, що відліки гребнів на окремих пальцях є генетично незалежними та не мають доказів на підтримку існування додаткових генів, що впливають на формування візерунка.

Інший спосіб успадкування візерунка відбитків пальців передбачає, що візерунок дуги на великому пальці та на інших пальцях успадковується як аутосомно-домінантна ознака. Подальші дослідження паттерну дуги припустили, що головний ген або багатофакторна спадковість відповідає за спадковість паттерна дуги.

Окрема модель для розвитку візерунка завитка вказує на те, що один ген або група зчеплених генів сприяє його успадкуванню. Крім того, успадкування візерунка завитка не виглядає симетричним, оскільки він, здавалося б, випадковим чином розподілений між десятьма пальцями даної особини. Загалом, порівняння шаблонів відбитків пальців лівої та правої рук свідчить про асиметрію у впливі генів на шаблони відбитків пальців, хоча це спостереження потребує подальшого аналізу.

На додаток до запропонованих моделей успадкування, певні гени були залучені як чинники формування візерунків на кінчиках пальців (їх точний механізм впливу на візерунки все ще досліджується). Багатофакторний аналіз зчеплення підрахунків пальців на окремих пальцях виявив зчеплення з хромосомою саме для безіменного, вказівного та середнього пальців. У мишей варіанти гена EVI1 корелювали з дерматогліфічними малюнками. Експресія EVI1 у людей безпосередньо не впливає на шаблони відбитків пальців, але впливає на формування кінцівок і пальців, що, у свою чергу, може відігравати певну роль у впливі на шаблони відбитків пальців. Дослідження повногеномних асоціацій виявили одиночний нуклеотидний поліморфізм у гені ADAMTS9-AS2 на, який, здавалося, вплинув на візерунок обертів на всіх пальцях. Цей ген кодує антисмислову РНК, яка може пригнічувати ADAMTS9, який експресується в шкірі. Модель того, як генетичні варіанти ADAMTS9-AS2 безпосередньо впливають на розвиток мутовка, ще не запропонована.

Ідентифікація за відбитками пальців, відома як дактилоскопія або ідентифікація за відбитками рук, — це процес порівняння двох відбитків шкіри від пальців рук або ніг людини, або навіть долоні або підошви стопи, щоб визначити, чи могли ці відбитки походити від однієї особи. Гнучкість фрикційної шкіри означає, що жодні відбитки пальців або долонь ніколи не будуть однакові в кожній деталі; навіть два відбитки, записані відразу один після одного з однієї руки, можуть дещо відрізнятися. Ідентифікація відбитків пальців, яка також називається індивідуалізацією, залучає експерта або експертну комп’ютерну систему, що працює за правилами порогової оцінки,

визначаючи, чи є два гребені тертя враження, ймовірно, походять від того самого пальця чи долоні (або пальця ноги чи підошви).

Навмисний запис хребтів вілбитку зазвичай робиться чорним чорнилом принтера, нанесеним на контрастний білий фон, як правило, на білу картку. Хребти також можна записати в цифровому вигляді, як правило, на скляній пластині, використовуючи техніку під назвою Live Scan.

«Прихований відбиток» — це випадковий запис хребтів, що залишилися на поверхні предмета або стіни. Приховані відбитки невидимі неозброєним оком, тоді як «патентні відбитки» або «пластикові відбитки» видно неозброєним оком. Приховані відбитки часто є фрагментарними і вимагають використання хімічних методів, порошку або альтернативних джерел світла, щоб зробити їх чіткими. Іноді звичайний яскравий ліхтарик зробить видимим прихований відбиток.

Коли фрикційні гребені стикаються з поверхнею, на якій буде зроблено відбиток, матеріал, що знаходиться на фрикційних гребнях, наприклад піт, масло, жир, чорнило або кров, буде перенесено на поверхню. Факторів, які впливають на якість відбитків, багато. Гнучкість шкіри, тиск осадження, ковзання, матеріал, з якого виготовлена поверхня, шорсткість поверхні та нанесена речовина – це лише деякі з різноманітних факторів, які можуть призвести до того, що прихований відбиток виглядатиме інакше, ніж будь-який відомий запис. Дійсно, умови, що оточують кожен випадок відкладення відбитку, є унікальними і ніколи не повторюються. З цих причин експерти відбитків пальців повинні пройти тривале навчання. Наукове дослідження відбитків пальців називається дерматогліфікою.

Відбитки пальців, зібрані на місці злочину або на доказах злочину, використовуються в криміналістиці для ідентифікації підозрюваних, жертв та інших осіб, які торкалися поверхні. Ідентифікація за відбитками пальців стала важливою системою в поліцейських органах наприкінці 19-го століття, коли вона замінила антропометричні вимірювання як більш надійний метод для ідентифікації осіб, які мають попередні записи, часто під вигаданим іменем, у сховищі судимостей.

Протягом останніх 100 років зняття відбитків пальців служило всім урядам у всьому світі для ідентифікації злочинців. Відбитки пальців є основним інструментом у кожному поліцейському відомстві для ідентифікації людей із кримінальним минулим.

Вчені, судді та засоби масової інформації оскаржили достовірність судово-медичних доказів відбитків пальців. У Сполучених Штатах дактилоскопісти не розробили єдиних стандартів для ідентифікації особи на основі відповідних відбитків пальців.

У деяких країнах, де відбитки пальців також використовуються в кримінальних розслідуваннях, спеціалісти, які перевіряють відбитки пальців, повинні зіставити кілька точок ідентифікації, перш ніж збіг буде прийнято. В Англії потрібно 16 точок ідентифікації, а у Франції – 12, щоб зіставити два відбитки пальців і ідентифікувати особу. Методи підрахунку балів були оскаржені деякими дослідниками відбитків пальців, оскільки вони зосереджені виключно на розташуванні певних характеристик у відбитках пальців, які потрібно зіставити.

Експерти по відбитку пальців також можуть підтримувати доктрину єдиної відмінності, яка стверджує, що якщо існує одна відмінність між двома відбитками пальців, вони не належать до одного пальця. Крім того, вчені стверджують, що частота помилок у зіставленні відбитків пальців не була належним чином вивчена. І було стверджено, що докази відбитків пальців не мають надійної статистичної основи. Було проведено дослідження щодо того, чи можуть експерти об’єктивно зосередитися на інформації про особливості у відбитках пальців, не вводячись в оману сторонньою інформацією, такою як контекст.

3 АЛГОРИТМИ ТА МЕТОДИ ВИДІЛЕННЯОЗНАК ЗОБРАЖЕННЯ

3.1 Система розпізнавання відбитків пальців на основі деталей

Вважається, що біометричне розпізнавання покращує перевірку особи. Використання біометричного розпізнавання також створює нові виклики для захисту конфіденційності суб’єкта та підвищує безпеку системи перевірки. Огляд літератури обговорює три основні категорії: систему відбитків пальців на основі деталей, схему виділення функцій і хешування зображень та методи захисту шаблонів.[8]

Розпізнавання відбитків пальців на основі деталей - популярний біометричний спосіб, який широко використовується в кількох програмах для розпізнавання особи, забезпечуючи унікальність і прийнятну продуктивність.

Система відбитків пальців на основі деталей включає три основні кроки:

- попередня обробка;
- виділення ознак;
- зіставлення.

Ця система вимагає зберігання наборів деталей у базі даних. Однак у кількох проектах було встановлено, що відбиток пальця можна відновити з інформації про деталі. Нещодавно кілька дослідників розглянули концепцію шаблону відбитків пальців. Автор запропонував новий підхід до шаблону відбитків пальців, сформувавши нове представлення деталей на основі спіральних кривих. Автори продемонстрували надійну схему обробки відбитків пальців, використовуючи структуру сусідства деталей і трикутники Делоне низького порядку. Цей алгоритм міг більш ефективно та методично шукати різні відбитки пальців у відповідній базі даних.

У роботі запропоновано метод захисту шаблону відбитків пальців, який перетворює набір точок деталей у бітовий рядок за допомогою техніки потрійного квантування (ТПК) на основі полярної сітки, яка забезпечує прийнятну швидкість розпізнавання. Крім того, автори використовували

дескриптор випадкової локальної області (ДВЛО) для створення вектора ознак фіксованої довжини. У цьому випадку характеристики ДВЛО витягуються з набору випадково та рівномірно згенерованих напрямних точок із зображення відбитка пальця. Крім того, запропоновано два дескриптори: дескриптор на основі текстури, який фіксує інформацію про орієнтацію та частоту деталей, і алгоритм зіставлення дескрипторів на основі деталей. Комбіновані дескриптори забезпечують високу дискримінаційну здатність.

Автори описали шаблон захисту конфіденційності для циліндрового коду контрольних даних (ЦККД), який забезпечує різноманітність, можливість відкликання та незворотності для дескрипторів ЦККД щодо оригінальних контрольних даних, з метою підвищення точності розпізнавання при зменшенні розміру шаблон.

Представлено метод симетричного хешування деталей відбитків пальців, спрямований на захист оригінального відбитка пальця та місця розташування деталей від зловмисника, тоді як автори запропонували схему, яка використовує надійне одностороннє перетворення, яке відображає геометричну конфігурацію точок деталей у кодовий вектор фіксованої довжини. Крім того, рекомендовано обробку відбитків пальців на основі чутливого до локації хешування (ЧЛХ) з використанням зменшених точок SIFT.

Автори підійшли до представлення спектральних деталей як вектора ознак фіксованої довжини для представлення набору деталей. Крім того, представилено новий алгоритм зіставлення відбитків пальців, який оцінює як деталі, так і гребені. Цей підхід використовується для пошуку перспективних початкових пар деталей.

Для кожної початкової пари контрольних точок було виконано процес зіставлення гребнів, який поступово узгоджував решту контрольних точок і гребнів. Крім того, описано ієрархічну систему відповідності, яка використовує ознаки на всіх трьох рівнях, а саме на рівні 1 (візерунок), рівні 2 (дрібні точки) і рівні 3 (пори та контури хребта).

Відносне зниження на 20% вирівняного коефіцієнта помилок (ВКП: швидкість, при якій помилки прийняття та відхилення є рівними; пристрій із найнижчим ВКП є найточнішим) системи узгодження, коли рівень 3 функції використовуються в поєднанні з функціями рівня 1 і рівня 2. Використовуючи інший метод, запропонувано цікавий підхід до перетворення ознак без вирівнювання.

Метою цієї методики є отримання спеціальної геометричної інформації з триплетів деталей для створення безпечного шаблону.

Запропоновано метод генерації шаблонів відбитків пальців, які можна скасувати, без вирівнювання, на додаток до методу створення змінних функцій. Щоб створити шаблони для кожної контрольної точки, значення інваріанта обертання та трансляції обчислюється з інформації про орієнтацію сусідньої локальної області, що оточує контрольні точки. Інваріантне значення використовується як вхід для двох змін функції, які виводять два значення для поступального та обертального рухів вихідних деталей, відповідно, у шаблоні, який можна скасовувати.

Також, запропоновано узгодження точкового шаблону для вирішення проблеми оптимального збігу між двоточковим шаблоном під час геометричної трансформації та шаблоном помилкових точок. Щоб підвищити стабільність і надійність зіставлення деталей, рекомендовано зіставляти деталі відбитків пальців за допомогою локальної та глобальної структур деталей. Однак система визначає особу користувача шляхом порівняння оцінки відповідності з пороговим значенням, встановленим адміністратором.

Представлено метод присвоєння оцінки кожній із вилучених деталей на основі кількох топографічних властивостей. Оцінка, пов’язана з деталізацією, означає її автентичність. Крім того, обгрунтовується розробка та впровадження онлайн системи верифікації відбитків пальців, яка працює в два етапи, наприклад, вилучення деталей і зіставлення деталей. Щоб знайти відповідність між деталями у вхідному зображенні та збереженому шаблоні, використовується алгоритм еластичного зіставлення на основі вирівнювання.

3.2 Методи вилучення функцій і хешування зображення

У вимогах до дизайну хешування зображень відбитків пальців надійність хешування зображень виникає завдяки надійному вилученню ознак і стисненню, що головним чином сприяє компактності остаточного хешу. Хеш повинен бути здатний справлятися з різними обробками зображень і геометричними атаками, якщо два схожі зображення, можливо, генерують майже однакове хеш-значення, інакше хеш-значення відрізняється від перцепційно різного зображення. У наведеній нижче літературі обговорюються різні схеми вилучення функцій і хешування зображень.

Автори створили «невід'ємну матричну факторізацію», яка є стійкою проти атак певного класу; включаючи розмиття, незначний додатковий шум і стиснення, хоча вона страждає від змін яскравості та великих геометричних трансформацій. Крім того, представлено поглиблений аналіз, перегляд і аналіз автентифікації зображень на основі вмісту;

У роботі викладено нову техніку класифікації зображень під назвою «хеш-функція зображення». Цей алгоритм використовує рандомізовані стратегії для необоротного стиснення зображень у випадкові двійкові рядки та є надійним проти обмеженого ряду атак. У роботі використовують випадкове перетворення для виділення ознак і аналізу основних компонентів, щоб зменшити довжину хешу, однак його надійність для зображення текстури обмежена. Крім того, автори відстоювали алгоритм для хешування зображень, заснований на контрольованій рандомізації за допомогою перетворення Фур'є, хоча алгоритм страждає від відомих атак, наприклад, адитивного шуму.

Було запропоновано виявлення віртуальних водяних знаків за допомогою оптимального мультиплікативного детектора водяних знаків. Він використовує псевдовипадково згенерований шаблон для вилучення хеш-бітів. Дослідники також представили аналіз безпеки перцептивного хешу зображення на основі факторизації невід'ємної матриці та показали, що використання секретного ключа в поєднанні з ключами, залежними від зображення, може підвищити безпеку. Крім того, у роботі пояснюється розкладання сингулярного значення

для хешування зображення; однак, цей алгоритм, хоча і є надійним, має обмежене зхастосування.

Відносно недавно запропонувано алгоритм хешування зображення з використанням візуально значущих ознак і виконано оцінку продуктивності та компроміси між геометричною інваріантністю та надійністю проти класичних атак. Крім того, створено новий алгоритм хешування зображення, з використанням локальної точки ознаки з *SIFT* для виявлення надійних ознак точок та включення критерію Гарріса для вибору найбільш стабільних точок, які є менш вразливими до атак обробки зображень.

У роботі приведено ефективну схему класифікація для системи ідентифікації відбитків долонь, яка використовує злиття результатів, отриманих за допомогою геометричного хешування на основі стратегії та оцінки SURF (прискорена надійна функція). Крім того, автори [] представили огляд детектора ознак. Огляд розкриває характерні властивості точок та їх інваріант при значних геометричних перетвореннях.

Автор проілюстрував метод вилучення відмінних інваріантних ознак із зображень, які можна використовувати для надійного зіставлення між різними видами об’єкта. Використовується алгоритм SIFT, оскільки він перетворює дані зображення в незмінні масштабні координати відносно місцевих об’єктів.

У роботі рекомендували схему автентифікації зображень на основі хешування, яка зосереджена на різних питаннях, таких як виявлення втручання, безпека та надійність. Секретний ключ використовується на етапі виділення ознак для випадкової модуляції пікселів зображення, щоб створити трансформований простір ознак. Схема, заснована на хеші, забезпечує хорошу стійкість до стиснення JPEG і фільтрації низьких і високих частот. Крім того, запропоновано два класи методів надійного хешування: системи хешування на основі випадкового хешування та хешування на основі вмісту, а також проведено аналіз безпеки для кожного класу, щоб продемонструвати, як виникають проблеми безпеки.

3.3 Методи захисту шаблонів

Захист шаблонів - це збірний термін для різноманітних методів, які спрямовані на збереження конфіденційності та покращення безпечного зберігання біометричних даних. Автори представили огляд схем захисту біометричних шаблонів і класифікували їх на підхід, заснований на трансформації і біометричні криптосистеми (див. рис. 1.8). Функції, які використовуються в підходах до трансформації, можуть спотворювати або рандомізувати біометричні дані так, що вихідні дані неможливо відновити з трансформованих шаблонів. Біометричні криптосистеми можуть бути вбудовані або генерувати секрети з біометричних даних.

Схема захисту біометричного шаблону має такі властивості:

- різноманітність, де безпечний шаблон не повинен дозволяти перехресне зіставлення в базі даних, забезпечуючи конфіденційність користувача;

- можливість відкликання, що скасовує скомпрометований шаблон і повторно випускає новий на основі тих самих біометричних даних;

- безпека, котра запобігає створенню зловмисником фізичної підробки біометричних ознак із викраденого шаблону;

- продуктивність, де схема біометричного шаблону не повинна погіршувати якість розпізнавання біометричної системи (частота справжніх позитивних результатів і частота помилкових позитивних результатів).

Автори окреслили сильні сторони автентифікації на основі біометрії у виявленні слабких ланок у системах, вказуючи на можливі атаки в загальній біометричній системі. Крім того, пояснено, що ефективність відповідності та безпека нечіткого сховища відбитків пальців покращується шляхом включення дескриптора деталей. Однак, у роботі запропоновано шаблон захисту для автентифікації на основі відбитків пальців, де алгоритм базується на допоміжних даних, що складаються з двох частин. Перша частина визначає надійні компоненти з високим співвідношення сигнал/шум у відбитку пальця, тоді як друга частина дозволяє корекцію шуму в квантованому представленні.

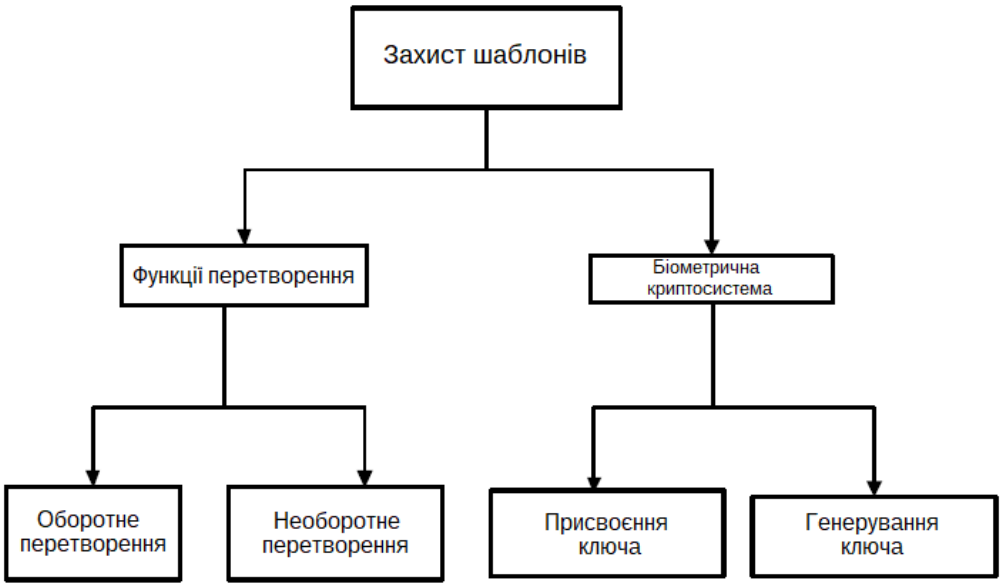

Рисунок 3.1 - Схеми захисту шаблонів

Автори окреслили сильні сторони автентифікації на основі біометрії у виявленні слабких ланок у системах, вказуючи на можливі атаки в загальній біометричній системі. Крім того, пояснено, що ефективність відповідності та безпека нечіткого сховища відбитків пальців покращується шляхом включення дескриптора деталей. Однак, у роботі запропоновано шаблон захисту для автентифікації на основі відбитків пальців, де алгоритм базується на допоміжних даних, що складаються з двох частин. Перша частина визначає надійні компоненти з високим співвідношення сигнал/шум у відбитку пальця, тоді як друга частина дозволяє корекцію шуму в квантованому представленні.

Автори описали вимоги до стандартизації архітектури зберігання та обробки біометричних даних, які задовольняють умовам відновлюваності (це властивості, які дозволяють системі відновлюватися після допоміжних даних): дані були скомпрометовані зловмисником; незворотність, незмінність (властивість двох або більше біометричних посилань між допоміжними даними та парами псевдонімних даних, завдяки якій вони не можуть бути пов’язані один з одним або з особою, від якої вони були отримані); конфіденційність і цілісність.

У роботі представлено шаблон зі змішаним ключем, який змішує шаблон користувача з секретним ключем для генерації іншої форми шаблону. Крім

того, запропоновано біометричний алгоритм шифрування для підключення та отримання цифрових ключів, який можна використовувати як метод безпечного керування криптографічними ключами. Автори досліджують зберігання біометричного шаблону обличчя за допомогою алгоритму захищеного ескізу та відзначають ефективність і безпеку методу захищеного ескізу. Також, проведено роботу з покращення безпеки шаблону, поєднавши біометричні дані вени руки з криптографією для створення нечіткого сховища. Викладено геометричне перетворення для захисту шаблонів відбитків пальців на основі деталей. Цей метод є надійним одностороннім перетворенням, яке відображає геометричну конфігурацію контрольних точок у кодовий вектор фіксованої довжини.

Створено нову техніку захисту відбитків пальців на основі коду циліндра деталізації (КЦД). Це гібридний метод, що поєднує трансформацію та ключ користувача, який забезпечує різноманітність, можливість відкликання та незворотність для дескрипторів КЦД щодо оригінальних деталей зображення відбитка пальця. Крім того, у роботі описано метод без вирівнювання для генерації шаблону, який використовує сусідні зв’язки навколо кожної контрольної точки.

Надають теоретичну основу, яка включає вимоги безпеки шаблонів, підходи до захисту та різні схеми захисту шаблонів відбитків пальців у деталях. У таблиці 3.3.1 наведено різні методи трансформації функцій відбитків пальців для схем захисту шаблонів.

Таблиця 3.1 - Методи, що використовуються для перетворення функцій відбитків пальців для захисту шаблону

Метод	Особливості	Результуюче представлення
Спектральні деталі	Деталі	Вектор
Біометричне шифрування	Зображення відбитка пальця	Вектор
Індикатор деталей	Деталі	Вектор
Гістограма трійки деталей	Деталі	Вектор
Прямокутна агрегація	Деталі	Вектор
Симетричний хеш	Деталі	Деталі
Дрібні структури	Деталі	Деталі

3.4 Дискретне перетворення зображень

Зі зростаючим попитом на покращену безпеку в нашому повсякденному житті, надійна особиста ідентифікація за допомогою біометричних даних зараз активно досліджується. Особу можна ефективно ідентифікувати за допомогою біометричних методів, таких як відбиток пальця, долоні та обличчя. Останнім часом багато дослідників запропонували кілька перспективних методів ідентифікації біометричних зображень з використанням доменів перетворення: дискретне перетворення Фур'є (ДПФ), дискретне косинусне перетворення (ДКП) і перетворення Фур'є-Мелліна (ПФМ) і дискретне Вейвлет-перетворення (ДВП).

Автори представили алгоритм виділення спектральних ознак для розпізнавання відбитків долонь. У цьому методі все зображення сегментується на кілька просторових модулів, і завдання виділення ознак виконується за допомогою двовимірного перетворення Фур'є. В цих просторових модулях демонструється висока точність розпізнавання та обчислювальна здатність.

У роботі представлено метод розпізнавання відбитків пальців на основі ознак ДКП. Застосовуючи ДКП-перетворення до дискретного зображення відбитка пальця, функції ДКП, які використовуються для зіставлення відбитків пальців, призводять до вищих показників розпізнавання та меншої складності. Було запропоновано схему розпізнавання відбитка долоні на основі ДКП, де

домінуючі спектральні характеристики виділяються окремо з кожної з вузьких смуг, що є результатом операції сегментації зображення.

Ця схема виділення ознак пропонує дві переваги:

- вона фіксує локальні варіації, які існують у зображеннях відбитків долонь, що відіграє важливу роль у розрізненні осіб;

- для завдання розпізнавання використовується простір ознак дуже низької розмірності, що забезпечує менше обчислювальне навантаження.

Авторами запропоновано метод розпізнавання часткового відбитка долоні, який поєднує в собі функції ПФМ та модифікованої фази – «Тільки кореляція». Крім того, у роботі представлено ефективну безпечну та надійну техніку хешування перцептивного зображення на основі перетворення Фур'є-Мелліна. Було показано, що цей метод стійкий до операцій обробки сигналів і геометричних атак. Було також показано, що функції на основі ПФМ перевершують хешування на основі декомпозиції сингулярного значення (ДСЗ) і вейвлетів за геометричних спотворень.

Перетворення Фур'є-Мелліна є важливим інструментом для розпізнавання образів, реконструкції та пошуку бази даних зображень, оскільки його результуючий спектр є інваріантним щодо обертання, трансляції та масштабування.

ПФМ можна розділити на три основні етапи, які призводять до стійкості щодо атак обертання, масштабування та трансляції:

а) перетворення Фур'є: перетворюється вихідне зображення в просторовій області в область спектру;

б) перетворення в логарифмічні полярні координати: перетворюються різниці масштабу та обертання на вертикальні та горизонтальні зміщення, значення яких можна вирахувати;

в) перетворення Мелліна: дає зображення простору трансформації, яке є інваріантним до обертання, масштабування та трансляції.

Дискретне косинусне перетворення намагається декорелювати дані зображення. Після декореляції кожен коефіцієнт перетворення може бути закодований незалежно без втрати ефективності стиснення.

Основні переваги ДКП полягають у тому, що він дає реальне вихідне зображення, та що це швидке перетворення. Основним використанням ДКП є стиснення зображень. Дійсно, після виконання ДКП можна відкинути коефіцієнти, що представляють високочастотні компоненти, до яких людське око не дуже чутливе. Таким чином, кількість даних може бути зменшена без серйозного впливу на те, як зображення сприймається людським оком.

Вейвлет-перетворення - це математичний інструмент, який дозволяє досліджувати сигнали та процеси генерування сигналів, що характеризуються нестаціонарною поведінкою. Він враховує еволюцію частотного вмісту сигналу в часі. Тут базис функцій генерується з однієї функції, що називається «материнським вейвлетом», змінюючи два параметри. Розташування вейвлета змінюється в часі або просторі зі зміною індексу. Це дозволяє розширенню чітко представляти розташування подій у часі чи просторі та забезпечує представлення деталей або роздільної здатності.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ

4.1 Дизайн та підхід реалізації

У літературі дослідники запропонували різні підходи для забезпечення найкращого рівня розпізнавання.

Наприклад, Джейн у 2001 році розробив нову техніку представлення на основі фільтра для розпізнавання відбитків пальців. Ця техніка використовує як локальні, так і глобальні характеристики зображення відбитка пальця для перевірки. Кожне зображення відбитка пальця фільтрується в кількох напрямках, а в центральній частині відбитка виділяється вектор ознак фіксованої довжини.

Етап узгодження обчислює відстань між вектором ознак шаблону (кодом пальця) та вхідним кодом пальця. У 2004 році використовували схему вилучення ознак на основі фільтра Габора для створення 384-вимірного вектора ознак для кожного зображення відбитка пальця.

Класифікація цих шаблонів виконується за допомогою нового двоетапного класифікатора, (KNN) діє як перший крок і знаходить два найбільш часто представлені класи серед K найближчих шаблонів, після чого відповідний класифікатор SVM вибирає найбільше підходящий клас двох.

6 SVM мають бути навчені для вирішення проблеми чотирьох класів, тобто всі SVM один проти одного. Використовуючи цю нову схему та працюючи над базою даних FVC 2000 (257 остаточних зображень), було досягнуто максимальної точності 98,81% із відсотком відхилення 1,95%.

У 2004 р. Запропоновано алгоритм покращення, заснований на аналізі Фур’є, який одночасно здатний отримувати локальну орієнтацію хребта, частоту хребта та показники якості хребта. [9]

Досліджено контекстну фільтрацію в області Фур’є на основі цих функцій. У 2007 році представили апаратну реалізацію, засновану на

модифікації булевого класифікатора k-найближчого сусіда (BKNN), запропонованого Газулою та Кабукою.

BKNN — це свого роду керований класифікатор, що використовує булеву нейронну мережу, яка має двійкові входи та виходи, цілі ваги, швидке навчання та класифікацію та гарантовану конвергенцію.

Особливість цього дизайну полягає в тому, що він реалізований на мікросхемі Field Programming Gate Array (FPGA). У 2014 році, представлено запропонований алгоритм ідентифікації за відбитками пальців, який використовувався генетичний алгоритм (GA) як інструмент вибору ознак для ідентифікації за відбитками пальців.

Запропонована система містить чотири основні кроки: попередню обробку, виділення ознак, вибір ознак і класифікацію. Підетапи попередньої обробки складаються з таких методів обробки зображень, як: покращення та сегментація.

4.2 Модуль попередньої обробки

Завдання цього модуля полягає в тому, щоб підготувати зображення FP для модуля вилучення функцій, а також покращити та підвищити якість FP, щоб позбутися від шуму, якщо він був, щоб він міг бути сумісним із продуктивністю системи. Цей модуль включає вдосконалення за допомогою фільтрації та сегментації аналізу домену Фур’є.

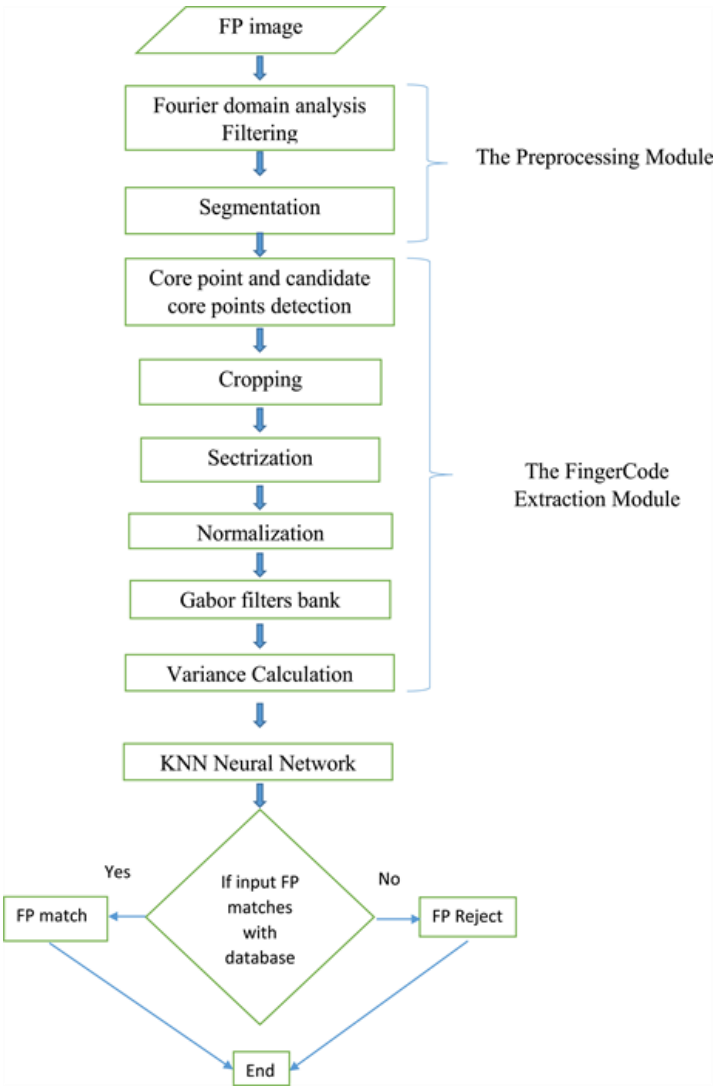

Рисунок 4.1 - ER-діаграма бази даних

Запропонована блок-схема системи розпізнавання FP. Фільтрація аналізу Фур'є-домену: ми вдосконалюємо FP-зображення, як у, за допомогою ряду кроків: аналіз у Фур'є-доміні, оцінка спрямованого поля, оцінка частоти хребта, енергетична карта та покращення.

В аналізі домену Фур'є локальну область зображення FP можна моделювати як поверхневу хвилю.

Нарешті, під час покращення зображення ділиться на блоки розміром 12 на 12, що перекриваються, із перекриттям у 6 пікселів між сусідніми блоками. Блок помножений на підняте косинусне вікно, щоб усунути будь-які артефакти через прямокутні вікна. Кожен блок фільтрується в частотній області шляхом

множення його на вибірковий фільтр орієнтації та частоти, параметри якого базуються на розрахунковій локальній частоті гребня та орієнтації.

Поблочні підходи мають проблеми навколо сингулярностей, де напрямок хребтів не можна апроксимувати одним значенням. Смугу пропускання спрямованого фільтра слід збільшити навколо цих областей. Зробивши смугу пропускання фільтра кусково-лінійною функцією відстані від сингулярностей. Спрямовану гістограму отримано при оцінці зображення орієнтації.[10]

Сегментація: у цій операції зображення є сегментованим, а фон відокремлений від зображення відбитка пальця. Це можна виконати за допомогою простого підходу поблокової дисперсії, оскільки фон зазвичай характеризується невеликою дисперсією. Зображення спочатку двійково закривається, потім розмивається (команда Matlab imerode), щоб уникнути дірок у зображенні відбитка пальця, а також небажаного ефекту на межі (між відбитком пальця та фоном). На рисунок 4.2 показано сегментоване зображення FP.

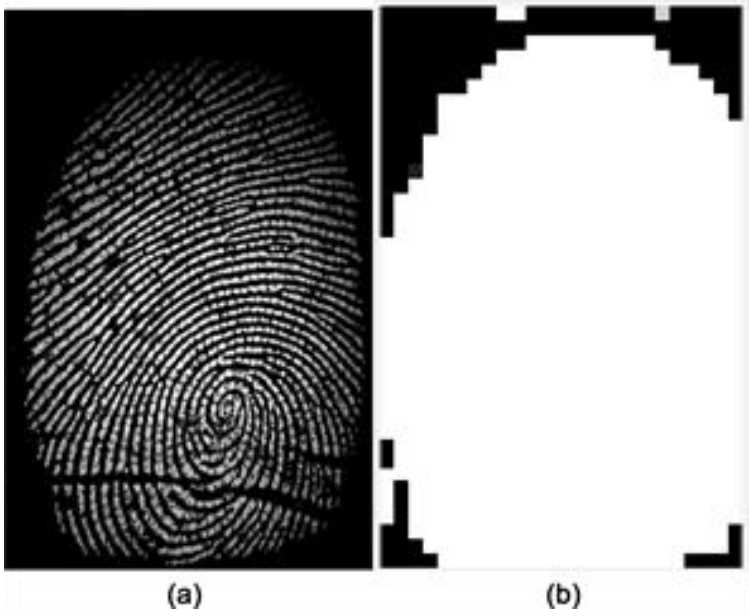

Рисунок 4.2 - сегментоване зображення FP.

4.3 Витяг функцій

Для кожної точки з основної та кандидатської базової точки буде реалізовано алгоритм filterbank_based. Рисунок 4.3 ілюструє структуру алгоритму на основі filterbank_based.

Виявлення основної точки та потенційних основних точок: основна точка визначається за допомогою кількох кроків:

1) Оцініть орієнтацію за розширеним зображенням FP, як описано.

2) Поле орієнтації використовується для отримання логічної матриці, де піксель має значення 1.

3) Після цього обчислення необхідно розрахувати результат комплексної фільтрації покращеного зображення відбитка пальця;

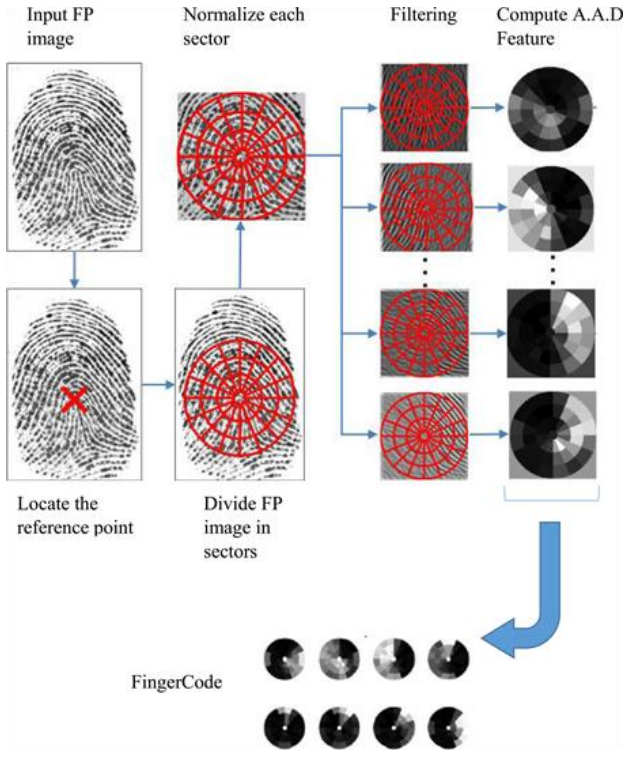

Рисунок 4.3 - Схема алгоритму на основі Filterbank.

Ми ідентифікуємо основні точки-кандидати за їх спеціальними властивостями симетрії. Таким чином, для виявлення основних точок-кандидатів застосовується складний фільтр, призначений для виявлення вилучення обертальної симетрії. Після обчислення виходу комплексної

фільтрації покращеного зображення відбитка пальця було знайдено максимальне значення виходу комплексної фільтрації, де пікселі логічного зображення встановлені на одиницю.

Дисперсія значень усіх пікселів у кожному секторі обчислюється після отримання 512 відфільтрованих зображень, що дає концентрацію хребтів відбитків пальців, що йдуть у кожному напрямку в цій частині відбиткає середнім абсолютним відхиленням від середнього значення, яке обчислюється за допомогою рівняння.

4.4 Зіставлення відбитків пальців за допомогою нейронної мережі KNN

Класифікація KNN є найпростішим методом у машинному навчанні. Якщо у вас є набір даних з міткою, і ви хочете класифікувати новий елемент, знайдіть у своєму наборі елементів, ті які є найближчими до бажаного.

Прогноз KNN обчислюється за допомогою функцій, зібраних у матрицях, у двоетапному процесі. На першому кроці ми обчислювали відстань між функціями в новому наборі даних (тестовий набір) і об’єктами в попередньому наборі даних (навчальні набори). На другому кроці вибираємо KNN і маємо найменшу відстань від набору відстані.

На етапі навчання основна точка та потенційні основні точки витягуються із зображення FP. Для кожної точки виділяється вектор ознак, тому зображення FP на етапі навчання матиме кілька векторів ознак залежно від кількості точок, які має зображення FP. Тому кожне зображення FP матиме різну кількість векторів ознак.

Одне зображення тренується для кожної людини, і цей процес буде повторено для всіх 90 осіб, які зберігаються в базі даних, і всі набір даних про функції зберігатимуться за межами нейронної мережі KNN.

Той самий процес для навчального зображення FP буде виконано на етапі тестування для тестового зображення FP. Основна точка та потенційні основні точки є витягом із тестового зображення FP. Для кожної точки виділяється вектор ознак, тому зображення FP на етапі тестування матиме кілька векторів

ознак залежно від кількості точок, які має зображення FP. Тому кожне зображення FP матиме різну кількість векторів ознак.

Другим кроком є обчислення відстані (яка буде евклідовою відстанню) між кожним вектором із вхідних векторів N і цілим числом векторів для всіх зображень FP у базі даних, а також визначення мінімальної відстані та збереження особи, яка це належати. Крім того, повторіть цей крок для всіх вхідних векторів N, і нарешті це буде N запропонованих осіб; особа, яка найбільше повторюється, буде кінцевим результатом відповідності ідентифікації.

Є 8 зображень для кожної людини, і одне зображення використовувалося для навчання, а 7 зображень для тестування, і це повторюється для всіх 90 осіб.

Якщо тестове зображення або невідоме вхідне зображення мають оцінку, вищу за вказане порогове значення, зображення буде прийнято, а в іншому випадку зображення буде відхилено.

Наприклад, ви можете вибрати такий високий поріг, що дійсно жоден самозванець не перевищить цей ліміт. У результаті жодні шаблони не сприймаються системою помилково. З іншого боку, шаблони клієнта з оцінками, нижчими за найвищі оцінки самозванців, хибно відхиляються. На противагу цьому ви можете вибрати такий низький поріг, щоб жоден шаблон клієнта не відхилявся помилково. Потім, з іншого боку, деякі шаблони самозванців хибно приймаються.

Якщо ви обираєте поріг десь між цими двома пунктами, відбуваються як помилкові відхилення, так і помилкові прийняття

Залежно від вибору балів порогового значення, між усіма або жодним із шаблонів самозванців не приймається системою помилково. Частка хибно прийнятих шаблонів, що залежить від порогу, поділена на кількість усіх шаблонів самозванців називається коефіцієнтом помилкового прийняття. Якщо надто високий пороговий показник застосовується до балів класифікації, деякі шаблони клієнта хибно відхиляються. Залежно від значення порогу, жоден або всі клієнтські шаблони будуть хибно відхилені.

Отже, ми з’ясували, що 70% поріг є найкращим порогом, який можна розглянути, оскільки він має хороший рівень розпізнавання для зображень FP, який становить 93,9683% у техніці зіставлення. Порівнюючи нашу роботу з іншими, вони також використовують k-найближчих сусідів (KNN), а база даних містить 28 осіб, 7 вибірок для кожної особи, а рівень розпізнавання досягає 98%, також використовують 257 остаточних зображень і досягнуто максимальної точності 98,81%, і ми використовуємо 90 осіб і 8 зразків для кожного і використовували один для навчання та 7 для тестування, тому було використано 720 тестових зображень і рівень розпізнавання був рівним до 93,9683%. Наш рівень розпізнавання нижчий, але ми використовуємо більшу базу даних, ніж вони, і щоразу, коли база даних велика, рівень помилок зростатиме.

ВИСНОВКИ

У цьому документі представлено дизайн і впровадження системи розпізнавання відбитків пальців з використанням алгоритму Filterbank_based для ряду основних точок і ключових точок-кандидатів на етапі виділення ознак і з використанням нейронних методів зіставлення KNN на етапі зіставлення та техніки порогового вибору. У ході виконання роботи було зроблено ряд висновків на основі практичних результатів, отриманих від впроваджених систем, і наступні є найважливішими з них:

1) Отриманно зображення відбитків пальців декількох осіб із нашої реальності різного віку та обертання зображення відбитків пальців, наскільки це можливо, означає, що кінцеві результати є більш реальними та застосовними.

2) Включення покращення зображення в систему ідентифікації відбитків пальців покращує якість вхідного зображення відбитків пальців, зменшує виділення хибних векторів ознак і мінімізує помилки зіставлення.

3) Алгоритм вилучення основних точок і потенційних основних точок є хорошим алгоритмом і підходить як основа для алгоритму вилучення ознак.

4) Алгоритм виділення ознак на основі алгоритму Filterbank_based створює хороший вектор ознак у порівнянні між відбитками пальців, що відрізняються від однієї людини до іншої.

5) Нейронні мережі KNN забезпечують відповідний результат відповідності, а 70% порогове значення методу забезпечує належні та хороші результати для зображень FP (90 осіб і 8 зразків для кожного), які належать до бази даних, що становить 93,9683% коефіцієнт розпізнавання.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fingerprint Source Book: manual of development techniques. Home Office, 2013.
2. Herschel W. J. The Origin of Finger-Printing. Oxford University Press. : навчальний посібник. 1916.
3. Fingerprint grip theory rejected. June 12, 2009. URL: http://news.bbc.co.uk/2/hi/health/8093134.stm.
4. Pierson D., Kantner J., Wester S. "Reconstructing sexual divisions of labor from fingerprints on Ancestral Puebloan pottery". 2019.
5. Jain R. Estimating fingerprint deformation. Proceedings of the International Conference on Biometric Authentication. 2004.
6. Kremen R. "Touchless 3-D Fingerprinting: A new system offers better speed and accuracy". 2009.
7. Ramotowski. Lee and Gaensslen's Advances in Fingerprint Technology / ed. by Robert. Public Safety Education Campus, 2013.
8. Bridges B. Practical Fingerprinting. Public Safety Education Campus, 1963.
9. Cowger J. F. Friction Ridge Skin: Comparisons and Identification of Fingerprints. Public Safety Education Campus, 1983.
10. Lee S. Advances in Biometrics: International Conference. Seoul : Proceedings. Springer Science & Business, 2007. 484 p.