Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

Зав.кафедрою БІСТ

Сергій РАССОМАХІН

«01» 12 2022 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Математична модель 3D-метрики для верифікації відбитків пальців»

оцінка « » Керівник д. т. н., доцент Рассомахін С.Г.

Голова ЕК Рецензент д.т.н., проф. Краснобаєв В.А.

Доценко С.І. _____ Виконавець : студент(ка) групи КБ-61

Прудиус Б.М.

Харків – 2022

РЕФЕРАТ

Пояснювальна записка містить: 60 сторінок, 24 рисунків, 2 таблиці, 11 джерел посилань, 1 додаток.

Об’єкт дослідження – відбиток пальця, алгоритм математичної моделі 3D-метрики на основі мінуцій.

Предмет досліджень – технології та методи проектування математичної моделі 3D-метрики на основі мінуцій.

Метою науково-дослідницької роботи є:

- теоретичний аналіз технологій зчитування відбитків пальця;
- теоретичний аналіз застосування алгоритму математичної моделі 3D-метрики у галузі кібербезпеки;
- теоретичний аналіз існуючих систем верифікації людини побіометричним данним;
- підведення підсумків та разробка алгоритму для будування математичної моделі 3D-метрики для верифікації відбитків пальців;

Ключові слова: БІОМЕТРІЯ, АУТЕНТИФІКАЦІЯ, ВІДБИТОК ПАЛЬЦЯ, АЛГОРИТМУ ДЛЯ БУДУВАННЯ МАТЕМАТИЧНОЇ МОДЕЛІ 3D-МЕТРИКИ.

ABSTRACT

The explanatory note contains: 60 pages, 24 figures, 2 tables, 11 sources of references, 1 addition.

The object of research is fingerprint, algorithm of mathematical model of 3D-metrics based on minutes.

Subject of research - technologies and methods of designing a mathematical model of 3D-metrics based on minutes.

The purpose of research work is:

- theoretical analysis of fingerprint reading technologies;
- theoretical analysis of the application of the algorithm of the mathematical model of 3D-metrics in the field of cybersecurity;
- theoretical analysis of existing human verification systems with biometric data;
- summarizing and developing an algorithm for building a mathematical model of 3D-metrics for fingerprint verification;

Key words: BIOMETRICS, AUTHENTICATION, FINGERPRINT, ALGORITHM FOR BUILDING A MATHEMATICAL MODEL OF 3D-METRICS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

SecurID -	(Також RSA SecurID) - технологія, розроблена компанією RSA, (згодом відома як RSA The Security Division of EMC) для надання двофакторної аутентифікації між користувачем і мережевими пристроями.
PIN-код -	(англ. Personal Identification Number - персональний ідентифікаційний номер) - аналог пароля
ID -	(англ. Data name, identifier - розпізнавальний знак) - унікальна ознака об'єкта
CMOS -	(complementary metal-oxide-semiconductor) - набір напівпровідникових технологій побудови інтегральних мікросхем і відповідна їй схемотехніка мікросхем.
CCD -	(«charge-coupled device») - спеціалізована аналогова інтегральна мікросхема, що складається з світлочутливих фотодіодів, виконана на основі кремнію.
FTIR -	(Інфрачервона спектроскопія з перетворенням Фур'є) - це метод, який використовується для отримання інфрачервоного спектра поглинання або випромінювання твердого тіла, рідини або газу.
ASIC -	(Application-specific integrated circuit, «інтегральна

	схема спеціального призначення») - інтегральна схема, спеціалізована для вирішення конкретного завдання.
ESD -	(Electronic Software Delivery) - електронне поширення програмного забезпечення. Електронна ліцензія являє собою ключ активації програмного продукту, який надсилається на електронну пошту після покупки.
NFC -	(«комунікація ближнього поля», «ближня безконтактна зв'язок») - технологія бездротової передачі даних малого радіусу дії.
JPEG -	(англ. Joint Photographic Experts Group, за назвою організації-розробника) - один з популярних растрових графічних форматів, застосовуваний для зберігання фотографій і подібних до них зображень.

ВСТУП

Деякі людські риси (наприклад, обличчя, голос, почерк) використовуються для розпізнавання людей у повсякденному житті. Однак за цими ознаками нам важко впізнати незнайомих або близьких людей. Біометричні системи - це системи автоматичного розпізнавання образів, які підтверджують і розпізнають людей на основі поведінкових (наприклад, хода, підпис, пульс) або біологічних (наприклад, відбитки пальців, обличчя, райдужна оболонка ока, вени) особливостей, і є одним із рішень, що допомагають ідентифікувати людей. Різноманітні біометричні системи вже давно розгорнуті і навіть використовуються в правоохоронних органах і комерційних додатках.

Біометрична аутентифікація з використанням відбитків пальців стала важливою темою досліджень у сфері інформаційної безпеки. На сьогоднішній день розроблено кілька алгоритмів для обробки зображень і поліпшення їхньої якості. Однак існує необхідність у розробці та реалізації алгоритмів з поліпшеною продуктивністю.

Цілями дипломного проєкту є вивчення біометричних систем автентифікації, аналіз переваг і недоліків кожної з них, вивчення матеріалів для зняття відбитків пальців і систем сканування відбитків пальців, а також розробка алгоритмів для побудови математичних 3D метричних моделей на основі мінуцій.

1 БІОМЕТРИЧНІ ТЕХНОЛОГІЇ

1.1 Біометрія

У міру зростання побоювань з приводу безпеки було розроблено та впроваджено цілу низку технологій для захисту організацій і користувачів та зменшення занепокоєння. Ці технології включають смарт-картки, антивірусне програмне забезпечення, біометричні дані, брандмауери, захищені паролем облікові записи та системи виявлення і запобігання вторгнень.

Підвищена увага до безпеки також відштовхує технології від людей у плані "простоти використання" операцій. Тому існує необхідність інтегрувати необхідні функції аутентифікації та управління в захист даних, інформації та "простоту використання". Біометрична технологія була показана як одна з інновацій, необхідних для досягнення цієї мети [1]. Автор однієї книги стверджує: "Біометрію можна визначити як автоматизований метод перевірки або розпізнавання особистості живої людини на основі фізіологічних або поведінкових характеристик, що ґрунтуються на чомусь, чим ми є або робимо.

На відміну від паролів, біометрична аутентифікація особистості значною мірою постійна і не може бути легко змінена. Цей тип аутентифікації не можна легко загубити, забути або передати іншим, як інші предмети, що використовуються для традиційної аутентифікації. Це пов'язано з тим, що люди часто мають унікальні фізіологічні або поведінкові характеристики.

1.2 Що таке біометрія?

Біометричні дані використовуються для ідентифікації особи або підтвердження її особи. Методи ідентифікації визначають особу суб'єкта шляхом порівняння біометричних зразків, раніше отриманих від суб'єкта та

збережених у базі даних. Для перевірки заявленої ідентичності використовуються методи аутентифікації, в яких порівнюються тільки збережені біометричні ознаки, що відповідають заявленій ідентичності [3]. Індустрія безпеки використовує три різні типи автентифікації.

- Відомі: пароль, PIN-код, персональні дані (наприклад, дівоче прізвище матері).
- Що у вас є: ключ-картка, смарт-картка, токен (наприклад, SecurID-картка).
- Те, що у вас є з народження: біометрія.

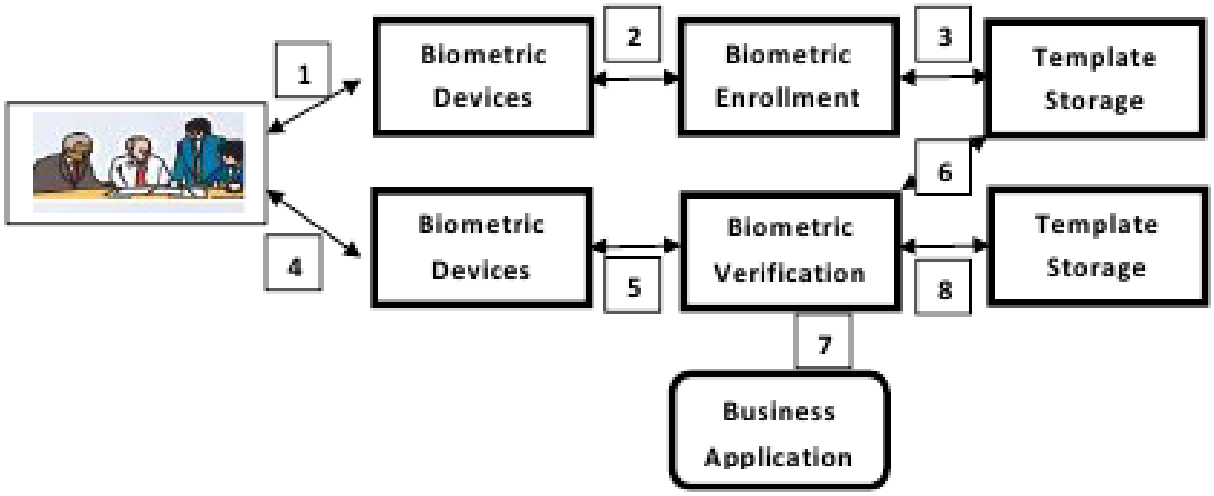


Рисунок 1.1 - Як працює біометрична система

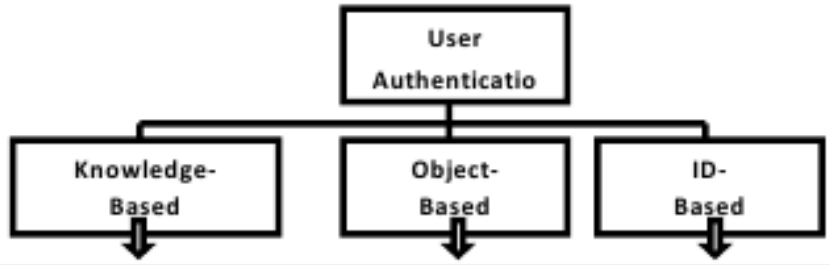
На думку Сільвермана, в роботі біометричної системи можна виділити вісім етапів, як показано на рисунку 2 вище [4], в тому числі.

1) Зняття окремих біометричних даних.
2) Обробка біометричної інформації, вилучення та реєстрація біометричних шаблонів.
3) Зберігати шаблон у локальному репозиторії, центральному репозиторії або портативному токені, наприклад, електронній картці.
4) Сканувати обрані біометричні дані в режимі реального часу

5) Обробка біометричних даних та отримання біометричного шаблону
6) Порівняти відсканований біометричний шаблон зі збереженим шаблоном
7) Обезпечити відповідність бізнес-додатків.
8) Підтримувати безпечний аудиторський слід використання системи..

1.3 Типи аутентифікації

Автор, О'Горман, вважає за краще використовувати мітки автентифікатора на основі знань, на основі об'єктів та на основі ідентифікації. Нижче для ілюстрації цього використовується рисунок 3 [5].



Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or Obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely Kept	Closely held	Forge-resistant
Example	**Traditional:**	Combination Lock	Metal key	Driver's license
	Digital:	Computer Password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

Рисунок 1.2 - Категорії аутентифікації користувачів

1) Аутентифікатори на основі знань ("що ви знаєте")

Аутентифікатори, засновані на знаннях, характеризуються неоднозначністю і секретністю. Прикладом такого типу є пароль, що запам'ятовується. До цього типу також відноситься інформація, яка є

прихованою, а не секретною. Ім'я вашого батька, улюблена машина тощо потрапляють до цієї категорії. Недоліком у цьому випадку є те, що конфіденційність аутентифікаційних даних зменшується при кожній їх передачі.

2) Об'єктно-орієнтовані автентифікатори (what-if автентифікатори)

Об'єктно-орієнтовані аутентифікатори характеризуються фізичним володінням. Фізичний ключ називається металевим. Основним недоліком металевих ключів від будинків є те, що в разі втрати вони можуть бути використані для проникнення в житло. Тому багато цифрових токенів також поєднують в собі інші елементи, такі як пов'язані паролі, наприклад, для захисту вкраденого або втраченого токена. Існує ще одна перевага використання фізичного токену для автентифікації. Якщо фізична річ втрачена, власник може побачити докази і діяти відповідно.

3) Аутентифікатори на основі ідентифікації особи ("хто ви")

Аутентифікатори на основі ідентифікації особи є унікальними для людини. Це стосується паспортів, університетських дипломів, кредитних карток, водійських посвідчень тощо. Те ж саме стосується біометричної інформації, такої як голос, сканування очей, відбитки пальців та підпис. Найкращим захистом як для документів, що посвідчують особу, так і для біометричної інформації є те, що їх важко скопіювати або підробити.

Багато біометричних технологій зараз використовуються на практиці, і багато нових технологій досліджуються і випробовуються в лабораторіях по всьому світу.

1.4 Біометричні техніки

1.4.1 Розпізнавання обличчя та вух

Розпізнавання обличчя може однозначно ідентифікувати особу за поєднанням декількох рис обличчя. Прикладами ознак, які можуть бути

використані, є форма носа та відстань між очима. Загалом на нашому обличчі налічується близько 80 різних особливостей, які в сукупності називаються вузловими точками. Біометричний шаблон, який використовується для автентифікації, базується на цих вузлових точках. Іноді для підвищення безпеки додаються особисті риси, такі як родимки.

До плюсів і мінусів розпізнавання облич можна віднести:

- Низька вартість - для мобільних пристроїв не потрібне додаткове обладнання, а для інших додатків камери не потрібні. Досить.
- Відстань - в залежності від мети, розпізнавання обличчя має ту перевагу, що його можна використовувати на значних відстанях, залишаючись непоміченим для людини, про яку йдеться.
- Вимагає гарного освітлення.
- Погана стабільність у часі: обличчя змінюються з віком та збільшенням або зменшенням ваги.
- Низький рівень безпеки: дуже легко обдурити системи розпізнавання осіб, використовуючи протези для зміни обличчя, що і відбувається на багатьох фотографіях.
- Високий відсоток відмов: низка факторів може завадити системі розпізнавання осіб отримати необхідний образ, наприклад, окуляри, головні убори, зачіска тощо. Вузлові точки, необхідні для аутентифікації.

Як і у випадку з іншими біометричними технологіями, вдосконалення відбувається з розробкою більш досконалих алгоритмів і методів розпізнавання облич.

Біометричною технологією, тісно пов'язаною з розпізнаванням обличчя, є розпізнавання вух, яке використовує численні нерівності та горбки на поверхні зовнішнього вуха як біометричні ознаки. Тонка будова вуха є не тільки унікальною, але й незмінною, оскільки зовнішній вигляд вуха зазвичай не змінюється протягом життя людини.

Існують системи розпізнавання вух, які працюють на основі 2D або 3D зображень вуха, які мають схожі переваги та недоліки з системами розпізнавання обличчя.

1.4.2 Відбиток пальців

Відбитки пальців є найстарішим і найпершим біометричним методом у сфері автентифікації особи; вони використовуються з 1896 року спеціально для ідентифікації злочинців. Основна ідея полягає в тому, що кінчик пальця хвилястий, з лініями, схожими на хребти, що проходять з одного боку пальця на інший. Хід цих хребтів безперервний і утворює візерунок. Характер течії породжує градаційні візерунки, такі як арки, петлі та завитки, тоді як нерівномірність течії в гребенях породжує характерні точки, які називаються мініатюрами, як показано на рисунку 5. [6]

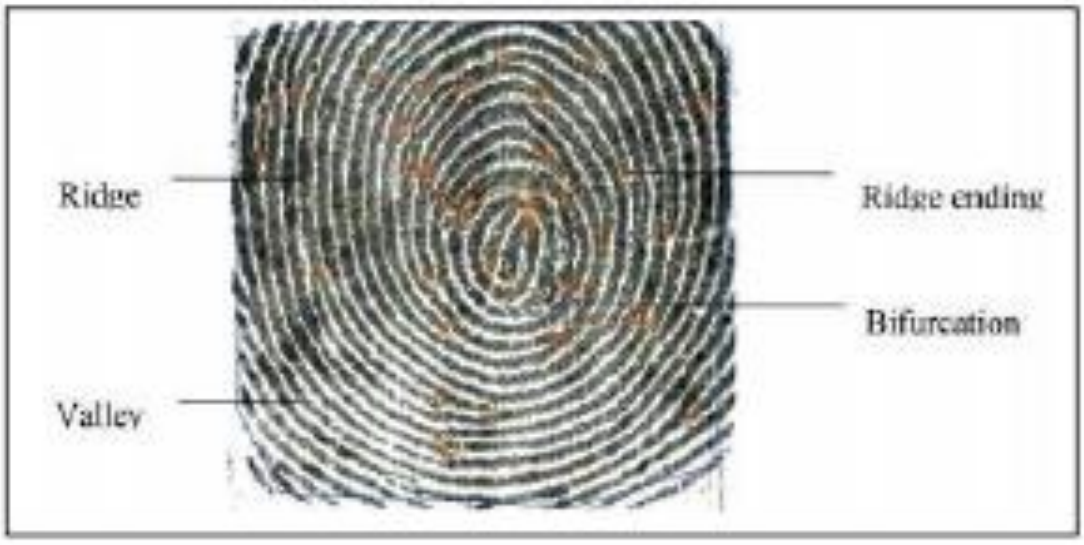


Рисунок 1.3 - Зразок зображення відбитка пальця

Дактилоскопічна ідентифікація, як правило, забезпечує достатньо високу точність як для ідентифікації, так і для ототожнення. Завдяки низькій вартості та компактним розмірам, вони дуже популярні для побутового використання. З іншого боку, якщо шкіра дуже суха або волога, датчик не може отримати зображення відбитків пальців прийнятної якості. Також для стабільної роботи датчика необхідно підтримувати його в чистоті.

1.4.3 Геометрія рук

Коли користувач кладе руку на потрібну поверхню, зображення руки фіксується камерою, яка знімає зверху. Рука користувача може бути вирівняна з контрольною міткою або штифтом. Як правило, на одному зображенні фіксуються два види: вид збоку і вид зверху. Боковий огляд зазвичай фіксується за допомогою верхньої камери та бокового дзеркала. Зображення кисті показує положення пальців та їх виміряну ширину, довжину, товщину і викривлення, а також їх відносну форму, див. Рис. 6.

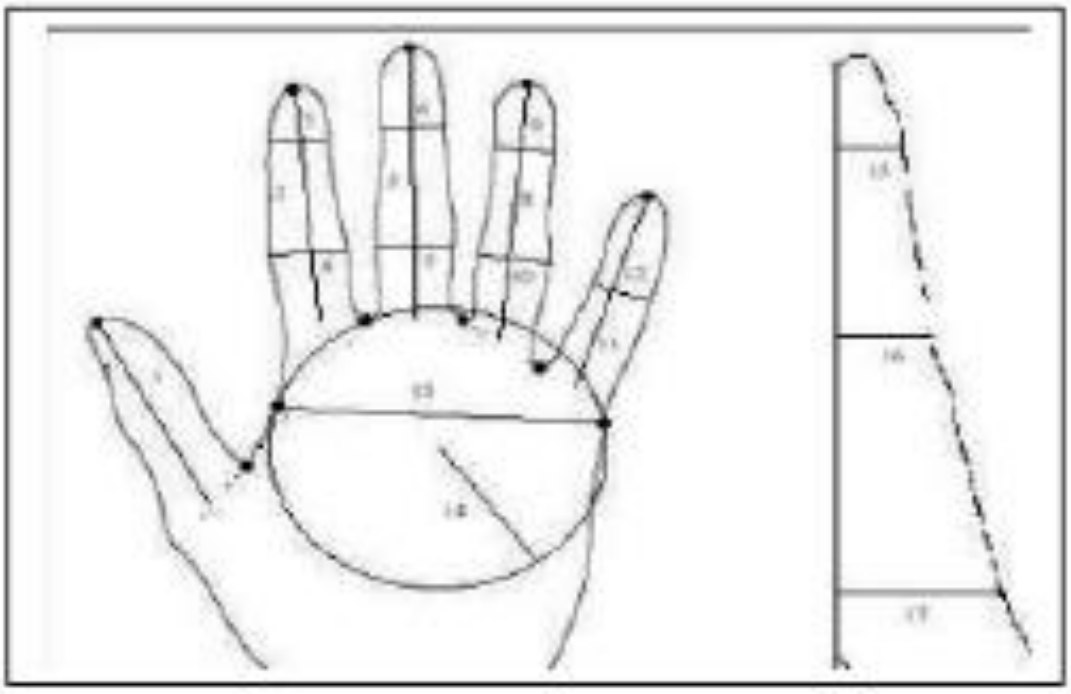


Рисунок 1.4 - Типові вимірювання геометрії кисті руки

У деяких випадках розмір шаблону геометрії кисті може бути дуже малим. У цьому випадку точність для валідації є прийнятною, але недостатньою для кращої ідентифікації. Головною перевагою системи є те, що вона є легкодоступною для багатьох людей і має хороший рівень сприйняття. Однак він досить громіздкий і має той недолік, що може бути

проблематичним для людей похилого віку та осіб з такими захворюваннями, як артрит.

1.4.3 Райдужна оболонка

Зображення райдужної оболонки зазвичай отримують за допомогою монохроматичних камер у видимому та ближньому інфрачервоному світлі (700-900 нм). Райдужка, кольорова частина ока, складається з тканини, яка називається трабекулярною сітківкою.

Коли райдужка розглядається зблизька, вона має багато шарів радіальних ліній або гратчастий візерунок. Видима сітчаста структура складається з таких елементів, як кільця, борозенки і дуги, які надають райдужній оболонці характерний візерунок. Висновок полягає в тому, що малюнок райдужної оболонки ока не залежить від генетичної структури і тому залишається незмінним протягом усього життя і навіть відрізняється між однояйцевими близнюками.

Рисунок 1.5 - Приклад сегментації райдужної оболонки з кодом райдужної оболонки у верхньому лівому куті

Розпізнавання райдужної оболонки ока дуже точне, може використовуватися як для зіставлення, так і для ідентифікації, і має дуже низький рівень помилкових спрацьовувань. чи можна легко перевірити приналежність райдужної оболонки ока живій людині. Швидкість ідентифікації також дуже висока. З іншого боку, витрати є відносно високими, а системи не є компактними. На них також впливає освітлення, відблиски і, в деяких випадках, окуляри, і вони можуть не підходити для маленьких дітей або людей з катарактою. Деякі системи візуалізації також потребують коротких періодів спокою.

1.4.4 Голос

Для розпізнавання голосу та аутентифікації використовується мікрофон, який записує голос людини. Для автентифікації записаний голос має бути оцифрований. Мова може промовлятися відомим користувачеві голосом (незалежна від тексту) або з текстом (залежна від тексту). В останньому випадку система може запропонувати або змінити текст. Текст можна читати як фрагментами, так і безперервно, як повний текст. Записана мова також покращується і виділяються індивідуальні особливості для створення мовних шаблонів.

Мова є поширеним засобом спілкування і в поєднанні з розгалуженою телефонною мережею та мікрофонами вартість розпізнавання мови може бути дуже низькою, а сама система може бути дуже компактною.

Крім того, він відносно простий у використанні. З іншого боку, голос змінюється з віком і може суттєво змінюватися від дитинства до юності. Крім того, на звук можуть впливати емоції, хвороби, акустика приміщення та навколишній шум. Невідповідність каналів (використання мікрофонів різного типу та якості) та відмінності між мікрофонами також є важливими проблемами для широкого використання цієї біометричної технології.

Таблиця 1.1 - Порівняння біометричних технологій

Biometrics	Univer-sality	Unique-ness	Perma-nence	Collecta-bility	Perfor-mance	Accepta-bility	Circumven-tion
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermo gram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L
H=High, M=Medium, L=Low							

У наведеній вище таблиці універсальність означає ступінь, до якого біометрична інформація є загальною для будь-якої особи, унікальність - ступінь, до якого біометрична інформація відрізняється від інших, стійкість - ступінь, до якого біометрична інформація не піддається впливу старіння, а збір - легкість, з якою біометрична інформація може бути отримана та оброблена. Ефективність - це точність, швидкість і надійність біометричної інформації; прийнятність - це ступінь, до якого технологія прийнята в повсякденному житті громадськості; а ухильність - це те, наскільки складно шахраям обійти або обдурити систему.

1.5 Майбутнє біометрії

З розвитком технологічних інновацій вартість впровадження біометрії має суттєво знизитися. Міжнародна біометрична група, що базується в Нью-Йорку, прогнозувала, що світові продажі біометрії зростуть з 2,1 млрд. доларів у 2006 році до 5,7 млрд. доларів у 2010 році[7], і саме це сталося[7], що сприяє широкому впровадженню її використання.

При впровадженні біометрії в охороні здоров'я необхідно також враховувати питання управління. При прийнятті рішення про впровадження

біометрії в організації необхідно розглянути та взяти до уваги низку питань, пов'язаних з біометрією.

1.5.1 Фізичні особливості людей

Чандра і Кальдерон, одні з авторів цієї книги, пояснюють, що не всі особи в організації мають поведінкові або фізіологічні характеристики, необхідні для використання біометричних систем [8]. У деяких випадках деякі користувачі біометричних систем можуть не мати достатніх або необхідних даних про відбитки пальців для їх точної обробки біометричним пристроєм. У цих випадках організації можуть зіткнутися з проблемою того, що деякі користувачі не мають достатньої або необхідної біометричної інформації, наприклад, за відбитками очей або пальців. У цих випадках організаціям, швидше за все, доведеться адаптуватися до конкретного користувача. Ці адаптації можуть суттєво збільшити витрати на впровадження, обслуговування та модернізацію біометричних технологій.

Ще одним викликом є непередбачувана зміна або еволюція фізіологічних характеристик, таких як старіння або втрата руки, пальця чи ока внаслідок операції або нещасного випадку. У цих випадках особа повинна повторно зареєструватися в програмі, що призводить до збільшення витрат.

Сектор охорони здоров'я, ймовірно, буде одним із секторів, який отримає найбільшу користь від біометричних технологій. Медичні заклади повинні будуть захищати медичну інформацію пацієнтів, спираючись на суворі державні та федеральні норми.

2 АУТЕНТИФІКАЦІЯ ЗА ВІДБИТКОМ ПАЛЬЦЯ

2.1 Відбитки пальців.

Відбитки пальців рук - це відбитки, що залишаються від тертя пальців рук людини. Гребені тертя (епідермальні гребені) - це видатні ділянки епідермісу пальців, долонь і підошов. Ці канавки підсилюють вібрації, що виникають, наприклад, коли кінчики пальців торкаються нерівних поверхонь, і допомагають передавати сигнали до сенсорних нервів, які визначають тонку текстуру. Канавки сприяють зчепленню на нерівних поверхнях та покращують контакт з дорожнім покриттям у вологих умовах. Епідермальні борозенки утворюють характерні візерунки, кожен з яких має свою індивідуальність, відомі як "мініатюри" в системах біометричної та дактилоскопічної ідентифікації. Ці дані є унікальними для кожної особи і тому можуть бути використані для аутентифікації та ідентифікації.

Існує три основних типи епідермального гребеня: вигнутий, кільцеподібний і закручений (рис. 9).

У людини найбільш поширені петлі (~65%), за ними йдуть завитки (~30%) і стрічки (~5%).

- Дуга: хребет входить з одного боку великого пальця стопи, піднімається посередині, утворюючи дугу, і виходить з іншого боку великого пальця стопи.

- Петля: виступ входить з одного боку пальця, утворює вигин і виходить з тієї ж сторони.

- Завивка: ребра утворюють коло навколо центру кінчика.

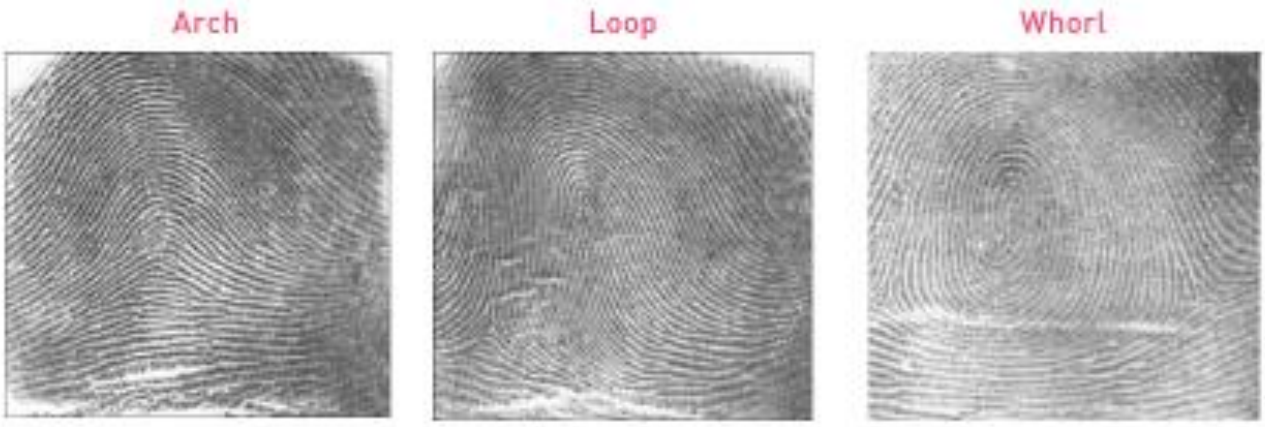


Рисунок 2.1 - Три основні типи зразків епідермісу. На фотографіях зображені "повнорозмірні" або "згорнуті" відбитки пальців.

Відбитки пальців мають інші особливості, окрім базової структури епітеліальних гребенів, як показано на рисунку 10.

Колючки починаються і закінчуються (кінчаються), перехрещуються (з'єднуються) і роз'єднуються (розгалужуються). В епідермісі також можуть визначатися невеликі ізольовані гребені (острівці), проміжки між гребенями (дельти) і окремі пори. Аналіз відповідності відбитків пальців зазвичай передбачає порівняння різних ознак зразка відбитків пальців. Успішне застосування тих чи інших технологій виявлення вимагає знання будови та властивостей шкіри людини.

Рисунок 2.2 - Інші типові функції пальців рук

Методи зіставлення відбитків пальців, що використовуються в системах автоматичного розпізнавання відбитків пальців, поділяються на дві основні категорії.

- засновані на мінуціях - у категорії "засновані на дрібницях

бере свій початок від ручного дактилоскопіювання, розробленого наприкінці 19 століття. Про це розповів сер Френсіс Галтон.

- Методи, що не базуються на мінуціях - методи, що не базуються на мініатюрах, застосовують широкий спектр принципів підгонки, від прямої кореляції субзображень до векторизації гребеня потоку та методів на основі частоти. Розмір датчика, тип і точка експлуатації (рівень FAR) визначають доцільність. Звичайно, інші системні ресурси, такі як доступна пам'ять і обчислювальна потужність, також важливі при виборі найкращого методу.

Алгоритми узгодження, які поєднують традиційні підходи, що базуються на маневрах, і підходи, що не базуються на маневрах, часто називають гібридними методами.

Гібридні рішення стають все більш популярними, оскільки датчики стають меншими, але не рідкість, коли навіть найменші датчики, такі як ті, що знаходяться в мобільних пристроях, взагалі втрачають деякі компоненти.

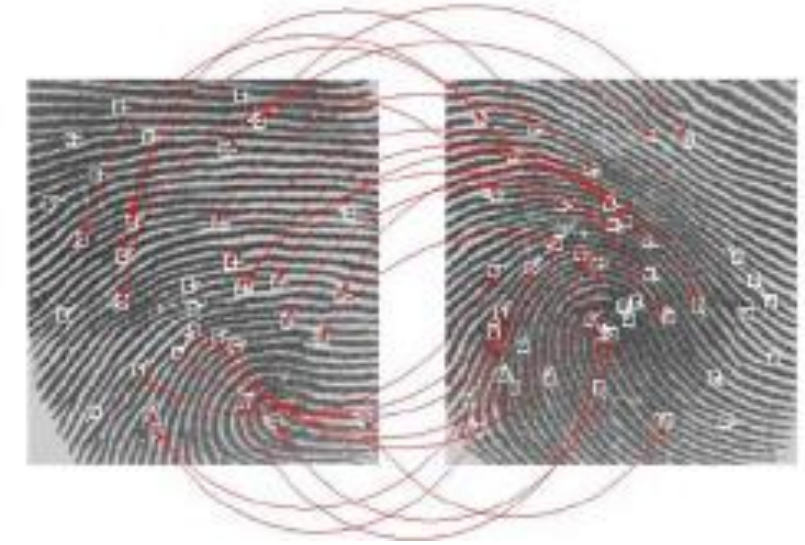


Рисунок 2.3 - Порівняння відбитків пальців на основі мінуцій

2.2. Датчики відбитків пальців

Дактилоскопічний датчик - це електронний пристрій, що використовується для отримання цифрового зображення зразка відбитків пальців рук. Зображення іноді називають активним зчитувачем відбитків пальців, а датчик може бути вхідним компонентом спеціального апаратного зчитувача відбитків пальців, але часто є просто частиною іншого пристрою, наприклад, мобільного телефону. Дактилоскопічний датчик фіксує відповідні характеристики відбитка пальця для подальшої обробки.

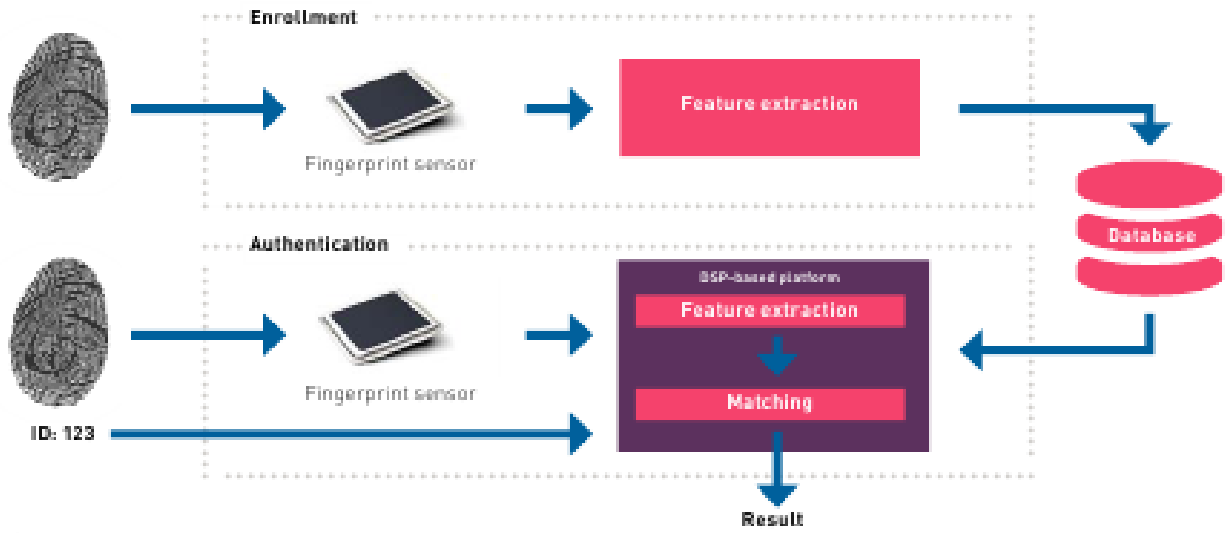


Рисунок 2.4 - Структурна схема системи автоматичного розпізнавання відбитків пальців.

Датчики відбитків пальців часто класифікуються як датчики відбитків пальців або сенсорні датчики, в залежності від того, як вони працюють. Дактилоскопічні датчики, часто вбудовані в ноутбуки, сканують відбитки пальців "по одному", коли палець проходить над датчиком, в той час як сенсорні датчики сканують весь відбиток пальця відразу. Датчики відбитків пальців, як правило, можуть бути меншими, ніж сенсорні датчики, що може знизити витрати, але, з іншого боку, мініатюризація може призвести до збільшення частоти помилкових відмов (FRR). Технології, проілюстровані на Рисунку 13, в основному використовують датчики відбитків пальців і тактильні датчики.

Рисунок 2.5 - Дактилоскопічні та сенсорні датчики

Перевагою дактилоскопічних датчиків є те, що вони можуть зчитувати більше даних, ніж сенсорні датчики, завдяки більшій площі поверхні, що полегшує подальший процес зіставлення. Однак, з точки зору користувача, сенсорна автентифікація є набагато швидшою, а отже, зручнішою в багатьох ситуаціях.

2.2.1 Оптичні датчики

Оптичні датчики вловлюють видиме світло і перетворюють його в електричний сигнал, а візерунок відбитків пальців фіксується у вигляді зображення. Датчик містить масив фотодіодних детекторів або фототранзисторів, які перетворюють енергію світла, що потрапляє на датчик, в електричний заряд. Більшість оптичних датчиків мають світлодіод або світлодіодний масив, який підсвічує кінчик пальця, з якого датчик знімає зображення відбитка пальця. Потім використовується призма із захисним покриттям для відбиття світла в напрямку датчика (рис. 14).

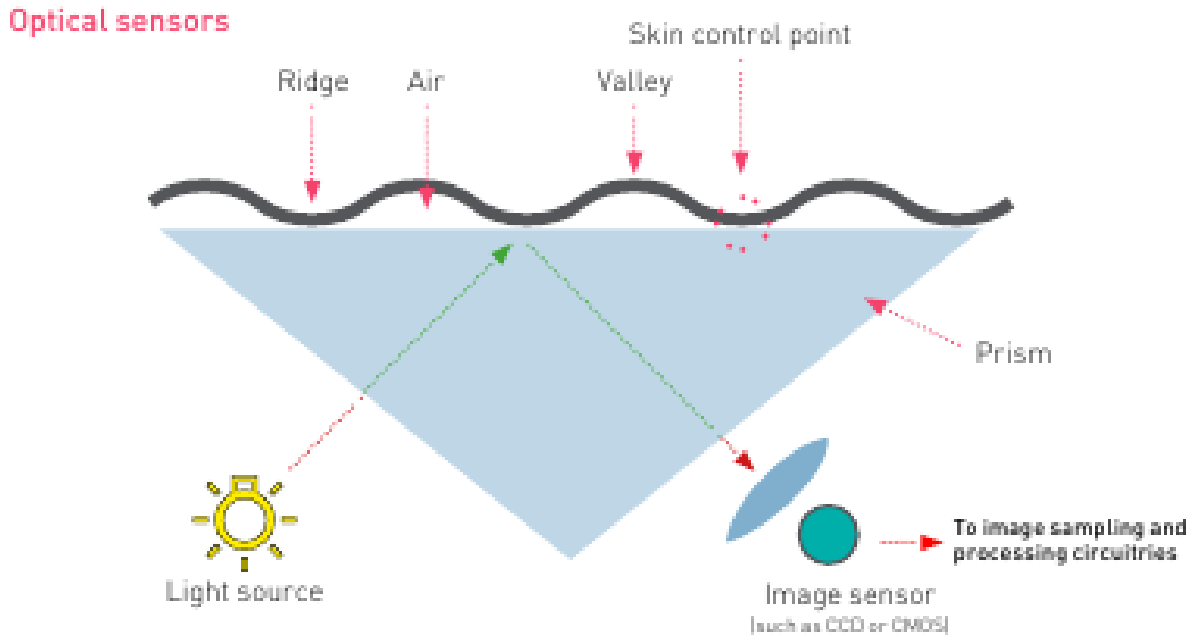


Рисунок 2.6 - Принцип роботи оптичних дактилоскопічних датчиків

Датчики, що використовуються в даний час в оптичних дактилоскопічних датчиках, включають ПЗЗ (прилади з зарядовим зв'язком) і КМОП-датчики. CCD та CMOS сенсори відносяться до того ж типу, що і ті, що використовуються в цифрових фотоапаратах; CCD сенсори особливо чутливі до низької інтенсивності світла, що робить їх придатними для передачі відтінків сірого кольору. Історично ПЗЗ детектори були набагато кращими за КМОП детектори, але за останнє десятиліття КМОП технологія значно покращилася і можливості КМОП технології наздогнали можливості ПЗЗ.

ПЗЗ набагато дорожчі у виробництві, ніж КМОП. Крім вартості, оптична візуалізація на основі КМОП має перевагу в тому, що частина логіки обробки зображення може бути змонтована на тому ж кремнієвому чипі, що і детектор. Тому більшість оптичних датчиків в побутовій електроніці, де важлива вартість і енергоспоживання, використовують КМОП детектори.

Оптичне захоплення було першим електронним датчиком відбитків пальців, який був прийнятий на озброєння, і є, мабуть, найпоширенішою

технологією. Їх головна перевага полягає в тому, що вони відносно дешеві, але вони мають і ряд недоліків.

- Дешево: оптичні датчики на основі КМОП можуть бути дешевими.

- Легко підробити: традиційне оптичне розпізнавання відбитків пальців відносно легко підробити, якщо використовується підроблений палець, але в багатьох випадках підроблений палець навіть не потрібен, достатньо хорошого зображення відбитка пальця. Більш досконалі оптичні сканери (FTIR) можуть бути менш схильні до підробки.

- Розмір: традиційні оптичні датчики, такі як лінзи та призми, є громіздкими і тому не підходять для встановлення в мобільні пристрої.

- Він також чутливий до розсіяного світла, масла, бруду, конденсату, льоду і навіть відбитків пальців, залишених іншими користувачами.

- Старіння: покриття призми і ПЗЗ-датчики можуть зношуватися з часом, знижуючи точність сканування в реальному часі.

Як і інші технології, оптичні сенсори також розвиваються, і для подолання проблем поводження з ними і забруднення були запропоновані різні рішення, в тому числі використання електрооптичних технологій і адаптивних камер. Однак, запропоновані рішення створюють різні проблеми і часто є дорогими. Крім того, розміри призми і системи лінз в споживчих пристроях, особливо мобільних, роблять матрицю неприйнятно великою, що стає все більш серйозним недоліком.

2.2.2 Ємнісні датчики

Ємність - це здатність утримувати електричний заряд. Ємнісні дактилоскопічні датчики використовують масиви з тисяч маленьких конденсаторних пластин для отримання зображення відбитка пальця.

Пластини матриці формують "пікселі" зображення. Кожна з паралельних пластин діє як пластина конденсатора, причому провідний шар шкіри пальця діє як інша пластина, а непровідний шар шкіри діє як діелектрик між ними. Коли палець прикладається до датчика, між виступами

пальця і пластиною датчика утворюється візерунок, який генерує слабкий електричний заряд. Від цього заряду датчик вимірює розвиток ємності досліджуваної поверхні. Вимірювання оцифровуються логікою датчика і надсилаються до розташованого поруч мікропроцесора для аналізу.

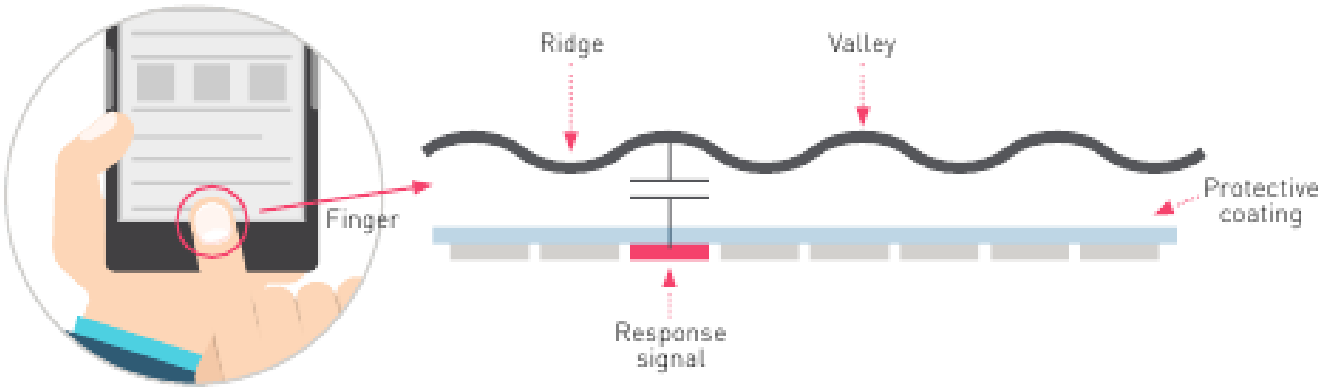


Рисунок 2.8 "Принцип ємнісного зчитування" Вимірювана ємність залежить від виступів і заглиблень відбитка пальця.

Ємнісний датчик неможливо обдурити якісною фотографією, а не реальним пальцем. Замість того, щоб створювати зображення нерівностей відбитка пальця, як це роблять оптичні сканери, датчик ємнісного сканера генерує складну схему електричних сигналів, які потім обробляються для отримання цифрового зображення відбитка пальця. Ємнісні сканери набагато важче обдурити, ніж оптичні, оскільки для створення зображення їм потрібен палець людини.

Ще однією перевагою ємнісних зчитувачів відбитків пальців є їх компактність, що дозволяє легко інтегрувати їх у портативні пристрої.

ASIC ємнісний дактилоскопічний датчик відбитків пальців

Датчики вимірювання ємності можуть бути виготовлені у вигляді спеціалізованих інтегральних схем (ASIC).

Інтегральні схеми (IC, "чіпи") - це тисячі або мільйони електронних компонентів, таких як датчики і транзистори, вбудовані в напівпровідниковий матеріал (кремній) і з'єднані між собою. Мікросхеми є дуже складними продуктами, але кожен компонент витравлюється на кремнієвій пластині за допомогою автоматизованого процесу фотолітографії. Тому їх виробничі витрати відносно низькі.

Найбільш поширеною технологією вимірювання активної ємності у виробництві ASICS є CMOS (комплементарний метал-оксид-напівпровідник). Перевагою цієї технології є те, що на одному кристалі можуть бути реалізовані як цифрова логіка, так і аналогові схеми; CMOS-технологія дозволяє інтегрувати аналогові функції і цифрові схеми на одному кристалі, в піксельних зрізах.

CMOS-технологія також має дві особливості, які є дуже важливими для дактилоскопічної ідентифікації: висока чутливість до шумів та низьке статичне енергоспоживання цифрових схем на основі CMOS-технології.

Сигнал, що вимірюється дактилоскопічним датчиком, є аналоговим. При цьому вихідний сигнал з датчика на біометричний мікропроцесор повинен бути цифровим. Тому необхідна схема для перетворення аналогового сигналу в цифровий в масиві сенсорних плат або поблизу нього. Цифрові дані, що надходять до мікропроцесора, є зображенням відбитка пальця. Відстані, виміряні на тисячах або десятках тисяч ємнісних піксельних пластин, представлені значеннями у відтінках сірого кожного пікселя на зображенні відбитка пальця. Подальша обробка зображення відбитків пальців дозволяє отримати детальне зображення відбитка пальця, включаючи тривимірні характеристики, для отримання більш тонкої інформації, необхідної для точної ідентифікації та автентифікації.

Переваги активних ємнісних дактилоскопічних датчиків.

Ємнісні датчики, особливо ті, що використовують активні методи вимірювання, описані вище, мають наступні важливі переваги в багатьох застосуваннях

- Відмінна якість зображення: розроблена для відмінної якості зображення, включаючи можливість зчитування 3D відбитків пальців, що забезпечує відмінну безпеку і стійкість до несанкціонованого доступу.

- Виявлення живих бактерій: може бути налаштований на реакцію тільки на живу тканину, що додатково знижує ризик фальсифікації.

- Невеликий і компактний розмір: легко інтегрується в портативні пристрої, такі як мобільні телефони та планшети.

- Низьке енергоспоживання: CMOS-процес, що використовується в сенсорних ASIC, забезпечує надзвичайно низьке енергоспоживання, що є додатковою перевагою в мобільних додатках.

- Швидкість - активні сенсорні датчики дозволяють зчитувати відбитки пальців одним рухом, без необхідності проводити зчитувачем.

- Стійкий і простий в установці: пластина датчика не вступає в прямий контакт з пальцями. Активні ємнісні датчики мають низькі втрати потужності, навіть при розміщенні за захисною кришкою або склом мобільних телефонів.

- Низька вартість - вартість кремнієвих сенсорів тісно пов'язана з розміром мікросхеми. Активні ємнісні датчики можуть бути мініатюризовані і, таким чином, вироблятися у великих кількостях за низькою вартістю.

Активні ємнісні датчики мають ряд недоліків. Чутливість до електростатичного розряду (ESD), проблема, спільна для всіх типів напівпровідникових ІС. Крім того, зі зменшенням розміру датчика стає все більш важливим, щоб запис і перевірка здійснювались ретельно і з найкращими алгоритмами узгодження. Ці вдосконалені алгоритми дозволяють виконувати більше циклів обробки і можуть збільшити енергоспоживання та вимоги до потужності використовуваного процесора.

2.2.3 Ультразвукові датчики

Ультразвукові дактилоскопічні датчики використовують принципи медичного ультразвуку для візуалізації відбитків пальців. На відміну від

оптичної візуалізації, ультразвукові датчики використовують дуже високочастотні звукові хвилі для проникнення в епітеліальний шар шкіри. Звукові хвилі генеруються п'єзоелектричним перетворювачем, а відбита енергія вимірюється п'єзоелектричним матеріалом.

Шар шкіри має такий самий характерний малюнок, як і відбиток пальця, тому, вимірюючи відбиті хвилі, можна отримати уявлення про відбиток пальця. Використання шкірного шару виключає необхідність очищення епітелію і поверхні датчика. Це дозволяє ультразвуковим датчикам добре зчитувати вологі або пошкоджені пальці та перевіряти їхню життєздатність. Оскільки сухість кінчиків пальців є поширеним явищем, лікарі можуть наносити гель на живіт перед проведенням УЗД, щоб побачити дитину.

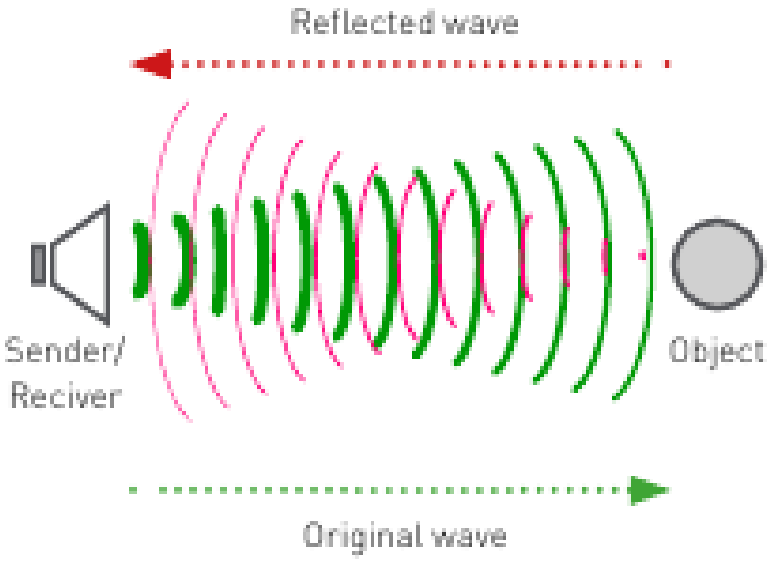


Рисунок 2.9 - Принцип ультразвукової дактилоскопії.

Ультразвукові датчики відбитків пальців мають перевагу в тому, що надають більше біометричної інформації, ніж багато інших датчиків відбитків пальців. З цією технологією були і залишаються значні проблеми. Він відносно повільний, дорогий, енергоємний, громіздкий (датчик має великі розміри) і вимагає великих обчислювальних потужностей через інтенсивне використання алгоритму.

2.2.4 Активні та теплові датчики температури

Термічні дактилоскопічні датчики отримують зображення відбитків пальців, вимірюючи температуру. В основі сенсора лежить масив пластин з піроелектричного матеріалу, що використовується у тепловізійних камерах. Коли палець торкається датчика, подовжувачі пальця контактують з поверхнею датчика і відбувається вимірювання температури. Потім вимірюється температура шкіри в місці проекції і температура навколишнього середовища кінчика пальця, щоб отримати зображення відбитка пальця.

Серйозні проблеми виникають з тепловими дактилоскопічними датчиками.

- У зв'язку з динамічним характером зміни температури, дактилоскопічні зображення

тимчасово, і стирається через десяті частки секунди, коли поверхня датчика досягає температури пальця.

- Чутливий до зносу і забруднень

- Коли температура навколишнього середовища наближається до температури поверхні пальця, датчик необхідно нагріти так, щоб різниця температур становила не менше 1°C, інакше різниця температур не може бути виміряна правильно і зображення відбитка пальця не може бути отримано.

Частину цих проблем можна вирішити за допомогою активних теплових датчиків. Активні теплові сенсори посилають теплові імпульси малої потужності на кожен піксель сенсора, коли палець щільно прикладається до поверхні сенсора. Тепловий імпульс перериває теплову рівновагу і забезпечує статичне зображення відбитка пальця.

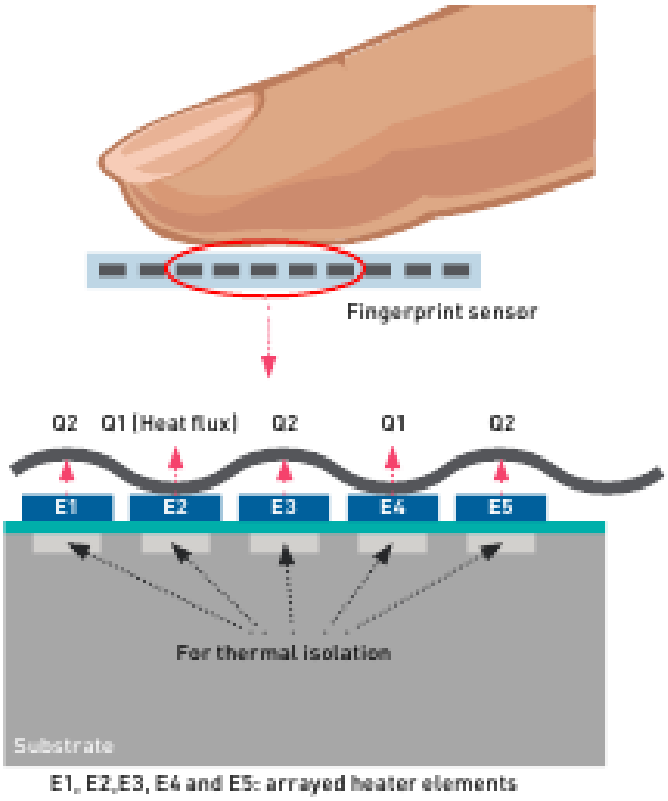


Рисунок 2.10 - Принцип активної теплової дактилоскопії.

Однак активна теплова технологія має і недоліки.

- високий попит на енергію

- Він вимагає більшої площі датчика і не може зафіксувати дрібні деталі, такі як піт.

- 3D-зображення не можуть бути створені.

2.2.5 Датчики, чутливі до тиску

Ця нова категорія дактилоскопічних датчиків використовує тонкоплівковий матеріал, який генерує електричний сигнал у відповідь на механічний вплив. Поверхня датчика виконана з дуже тонкого, гнучкого і непровідного діелектричного матеріалу. Коли палець прикладається до датчика, поверхня піддається різному тиску через нерівності, що призводить до різної кількості електричного струму, який може бути виміряний для отримання зображення відбитка пальця.

Чутливі до тиску датчики можуть бути мініатюрними і є однією з небагатьох категорій датчиків, окрім ємнісних, які можуть бути інтегровані в мобільні пристрої, такі як мобільні телефони та планшети. Однак, існуючі датчики чутливі до температури і не підходять для використання в суворих або мінливих умовах навколишнього середовища.

2.3 Порівняння технологій дактилоскопічних датчиків

Є кілька важливих факторів, які слід враховувати при виборі найбільш підходящої технології або фізичного датчика відбитків пальців для конкретного продукту, програми або процесу. Вибір технології залежить від таких параметрів продуктивності, як якість зображення, швидкість і енергоспоживання. Під час фактичної розробки продукту необхідно враховувати інші параметри, такі як розмір датчика, вартість та варіанти упаковки.

Ось основні міркування, які слід враховувати при виборі найкращого дактилоскопічного датчика та технології.

2.3.1 Якість та роздільна здатність зображення

Якість зображення, яке отримують дактилоскопічні датчики, є основоположним і важливим параметром. Краща якість зображення дозволяє використовувати менші датчики, які фіксують більше деталей на одиницю площі, що зменшує витрати. Якість зображення залежить від здатності датчика виявляти слабкі сигнали та усувати небажані шуми. По можливості, відбитки пальців не слід "виставляти напоказ" протягом тривалого та нудного періоду часу. Якість зображення може бути виміряна різними способами, але загальним параметром в системах розпізнавання відбитків пальців є показник FTE (Failure to Enroll); показник FTE - це відсоток випадків, коли датчик не може зчитати біометричний ідентифікатор в обсязі, необхідному для продовження обробки та реєстрації користувача.

Помилки при зчитуванні відбитків пальців також можуть виникати через вологість шкіри, подряпини або сторонні шуми, що потрапляють в

систему розпізнавання голосу. Інша часто використовувана метрика - dpi (точок на дюйм), яка вказує на роздільну здатність датчика. Якщо роздільна здатність низька (низька роздільна здатність на дюйм), дрібні деталі не можуть бути зафіксовані, що призводить до низької якості зображення. За допомогою ультразвукових та активних ємнісних датчиків тепер можна досягти відмінної якості зображення, зчитуючи шар шкіри, який є більш чітким і менш спотвореним, ніж зовнішній шар шкіри. Активні ємнісні датчики також можуть бути оснащені власною електронною схемою в кожному пікселі.

Наразі стандартна роздільна здатність активних ємнісних датчиків становить 508 dpi, що також відповідає специфікаціям американського стандарту ANSI/NIST.

2.3.2 Швидкість

Швидкість роботи системи дактилоскопічної ідентифікації має великий вплив на зручність її використання. Для реалізації високошвидкісного датчика аналого-цифрове перетворення та обчислення, необхідні для ідентифікації відбитків пальців електронними схемами ASIC, повинні бути ефективними. Для досягнення бажаних характеристик важливо писати алгоритми в мінімалістичному стилі.

У додатках, що використовують спеціальні біометричні процесори, процес автентифікації може бути дуже швидким і точним, оскільки обчислювально інтенсивна частина алгоритму виконується на апаратному забезпеченні. У додатках, де алгоритми працюють на основному процесорі, таких як мобільні телефони, ефективні алгоритми є ключем до швидкої автентифікації.

Швидкість також залежить від того, чи виконує система датчиків автентифікацію 1:1 або 1:n. Аутентифікація може давати більш швидкі результати, ніж системи перевірки особи, оскільки вона лише порівнює захоплене зображення зі збереженим шаблоном. Ще одним аспектом, який

визначає швидкість роботи системи, є час, необхідний для підготовки датчика до зчитування.

Ємнісні датчики, датчики температури та тиску можуть бути використані дуже швидко. На даному етапі час запуску та тестування цих датчиків може становити менше 500 мс.

2.3.3 Споживання енергії

У портативних додатках, таких як мобільні телефони і смарт-карти, енергоспоживання сенсорної системи є критичним і важливим фактором. Високе енергоспоживання не тільки розряджає батареї пристрою, але й генерує тепло, яке може пошкодити батарею та інші елементи живлення.

Важливо враховувати тимчасове енергоспоживання датчика, тобто кількість енергії, яка фактично використовується датчиком в процесі роботи. Наприклад, сенсор мобільного телефону активний приблизно на одну секунду 20 разів на день і неактивний протягом решти 24 годин. На час роботи від батареї явно більше впливає енергоспоживання режиму очікування (холостого ходу), ніж енергоспоживання активного датчика.

Енергоспоживання визначається як апаратним, так і програмним забезпеченням сенсорної системи; CMOS-сенсори часто є малопотужними, оскільки вони споживають значну енергію лише під час перемикання транзисторів, тобто під час сканування пальця. Розмір датчика також впливає на енергоспоживання: менші датчики споживають менше енергії. Детальна електрична конструкція датчика також має значний вплив на енергоспоживання.

Менші датчики споживають менше апаратної потужності, але, як правило, мають менше ємнісних піксельних пластин, тому площа пальця на зображенні менша. Для запису та автентифікації менших зображень з достатньою деталізацією потрібні більш досконалі та якісні алгоритми. Вища якість зображення та складніші алгоритми вимагають більшої обчислювальної потужності, що може призвести до більшого

енергоспоживання. Цей ефект компенсується меншим енергоспоживанням датчиків меншого розміру, тому важливо мати високоефективні алгоритми обробки та автентифікації зображень відбитків пальців.

Ємнісні датчики споживають менше енергії, ніж будь-які інші датчики, представлені на ринку. Оптичні, ультразвукові та теплові датчики потребують більшої потужності і тому менш придатні для мобільних застосувань.

Типове споживання активних ємнісних датчиків становить 5 мкА в режимі холостого ходу і 20 мА під час роботи.

2.3.4 Розмір

Особливо в мобільних додатках розмір, а точніше маленький розмір, часто є вирішальним параметром при виборі дактилоскопічного датчика. У мобільних телефонах, планшетах і фотоапаратах простір для розміщення всіх необхідних компонентів обмежений, а зовнішня частина пристрою вже може бути захаращена дисплеями, іншими кнопками, пластинами і т.д. Невеликі ASIC також є більш економічно ефективними, ніж великі датчики, оскільки вони використовують менше кремнію і дешевші у виробництві.

Однак, в додатках для розпізнавання відбитків пальців існує компроміс між розміром і якістю зображення. Занадто малі датчики і занадто низька роздільна здатність призводять до низької якості зображення, що, в свою чергу, вимагає більш складних і енергоємних алгоритмів зіставлення, що ускладнює або унеможливлює безпечну реєстрацію та автентифікацію.

Активні ємнісні датчики зазвичай мають розмір від 84 х 84 мм до 160 х 160 мм і можуть мати круглу, прямокутну або будь-яку іншу двовимірну форму за бажанням розробника продукту.

2.3.5 Вартість

Вартість є важливим фактором при виборі сенсорної системи. Все більш важливим стає сприяння впровадженню ідентифікації за відбитками

пальців у секторах масового виробництва, де потрібні недорогі компоненти, такі як мобільні телефони та смарт-картки.

Вартість активних дактилоскопічних датчиків на основі кремнію тісно пов'язана з розміром датчика, оскільки матеріал є основним фактором вартості. На вартість також впливає виробничий процес, системна інтеграція та технологія, що використовується.

2.3.6 Упаковка та інші варіанти дизайну

Датчики відбитків пальців повинні бути вбудовані в кінцевий продукт таким чином, щоб доповнювати і розширювати його функціональність, не обмежуючи дизайн оригінального продукту. Виробники смартфонів конкурують не лише за функціональність, а й за дизайн. Виробники автомобілів не йдуть на компроміси в дизайні інтер'єру і хочуть, щоб їх датчики ідеально вписувалися в салон автомобіля. Датчики в системах контролю доступу повинні витримувати незліченну кількість циклів використання та суворі погодні умови.

Для того, щоб виконати вищезгадані конструктивні вимоги, дуже важливо враховувати упаковку і захисне покриття датчика. Основною перевагою активних ємнісних систем є те, що вони можуть фіксувати відбитки пальців через матеріали, які використовуються для інкапсуляції кінцевого продукту, наприклад, скло. Однак датчики, які фіксують відбитки пальців через 400-мікронне скло або кольорову кераміку, повинні виявляти дуже слабкі сигнали. Для цього потрібні ефективні алгоритми підсилення сигналу, вдосконалена обробка сигналу та подальші процеси узгодження всередині датчика.

Якщо кінцевий продукт включає в себе датчик відбитків пальців, інші функції також є важливими. Датчик повинен мати фізичні, електричні та логічні інтерфейси для завершення виробу. Необхідно вирішити, чи повинен алгоритм зіставлення працювати на окремому біометричному процесорі або на хост-процесорі продукту. Якщо використовується хост-процесор, іншими

важливими параметрами для проектування є те, чи надає постачальник датчика алгоритми для конкретної операційної системи, чи може він працювати в безпечному середовищі і чи може він шифрувати критичні дані.

2.3.7 Безпека та комфорт

Розділ 2.3 описує елементи безпеки та зручності автоматизованих систем автентифікації та способи їх вимірювання, а також визначає коефіцієнт помилкового прийняття (FAR) та коефіцієнт помилкової відмови (FRR). Існує залежність між безпекою та зручністю: чим безпечніша (сильніша) автентифікація, тим більше потрібно збирати та аналізувати даних, що, в свою чергу, вимагає більше часу та співпраці з боку особи, яка автентифікується, та спричиняє незручності.

Різні технології розпізнавання відбитків пальців показують різні криві FRR і FAR, в залежності від продуктивності датчика, обробки зображення і використовуваного алгоритму зіставлення. Як завжди, доводиться шукати компроміс між вартістю (в даному випадку розміром і потужністю датчика) і формою кривої FRR в порівнянні з кривою FAR. Однак, коли вдосконалені активні ємнісні датчики поєднуються з відповідними алгоритмами, невеликі датчики в мобільних пристроях можуть досягати FAR 100 000, зберігаючи при цьому FRR близько 1%. Таким чином, активні ємнісні датчики є однією з найпростіших сенсорних технологій на сьогоднішній день.

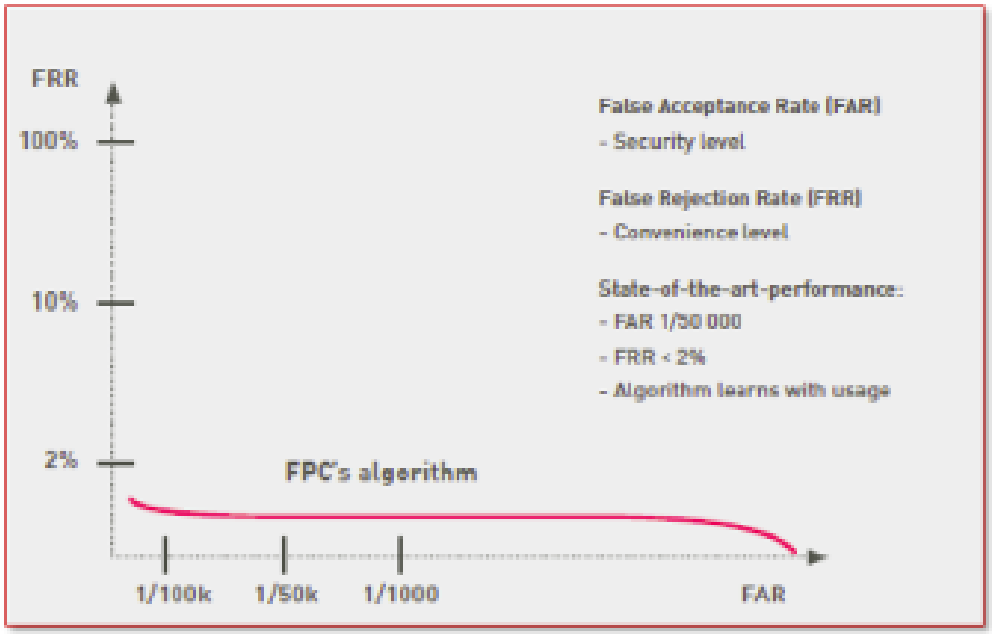


Рисунок 2.11 - Типова крива FRR в порівнянні з FAR для сучасних активних дактилоскопічних датчиків (крива DET - крива граничної помилки виявлення).

Таблиця 2 - Порівняння технологій дактилоскопічної ідентифікації

	Active Capacitive	**Capacitive**	**Ultrasonic**	**Optic**	**Active Thermal**
Cost efficiency	75	50	25	50	50
Design flexibility	100	25	75	25	25
Technology maturity	100	100	75	100	50
Security	75	25	100	25	50
Convenience	100	50	100	25	25
Power efficiency	100	75	50	50	0
Mobile device adoption	100	0	25	50	0
100 Very high 75 High 50 Medium 25 Low 0 Very low					

2.4 Відбитки пальців та їх порівняння

Дві найважливіші операції в системах біометричної автентифікації - це реєстрація та автентифікація. З автентифікацією за відбитками пальців обидві операції можна зробити більш зручними за допомогою відповідних допоміжних заходів, таких як механічні інструкції для користувача щодо правильного розміщення пальця на датчику або інтелектуальний користувальницький інтерфейс, який керує процесом реєстрації. Якщо датчик відбитків пальців встановлюється на об'єкті, який не має функції введення/виведення, наприклад, на кредитній картці, він повинен підтримувати додаткові функції, такі як зв'язок ближнього поля (NFC) зі смартфоном.

Зображення відбитків пальців рук, зафіксоване датчиком, є монохромним цифровим зображенням, тобто таким же, як і зображення цифрової камери, але тільки з відтінками сірого зображення відбитка пальця. Для забезпечення реєстрації та подальшого зіставлення, отримане зображення повинно бути покращено шляхом попередньої обробки перед тим, як ознаки відбитків пальців будуть вилучені та використані в процесі зіставлення. Обробка зображень, виділення ознак і зіставлення зазвичай називають алгоритмами розпізнавання відбитків пальців.

2.4.1 Попередня обробка, виділення ознак та шаблонування

Розрядність оригінального зображення відбитків пальців у відтінках сірого зазвичай становить 8 біт і, в залежності від розміру датчика, кожне з цих зображень вимагає декількох мегабайт пам'яті, хоча методи стиснення без втрат і з втратами, такі як JPEG, можуть стискати зображення щонайменше в десять разів. Кожне зображення все одно займає місце в пам'яті. З цієї причини для співставлення використовуються ознаки відбитків пальців, а не все зображення. Оцифровані елементи займають менше місця в

пам'яті і, що більш важливо, вимагають менш складних алгоритмів зіставлення, ніж повне зображення.

Першим етапом аналізу є отримання максимально чистого зразка відбитків пальців, використовуючи методи обробки зображень. Для зображень у відтінках сірого цього можна досягти, опускаючи яскраві ділянки.

Об'єкти темніші за поріг - чорні. Для отримання висококонтрастних зображень відбитків пальців також можуть використовуватися вдосконалені алгоритми покращення, засновані на напрямку та частоті відбитків пальців.

При використанні з'єднання на основі контрольно-пропускних пунктів наступним кроком є визначення та знаходження цих пунктів. Наприклад, кінцева точка лінії і початкова точка перехрестя утворюють тонкий перетин. Після ідентифікації контрольно-пропускного пункту його положення фіксується як відстань від центру (серцевини) траси. Крім положення контрольної точки, часто фіксується також кут нахилу контрольної точки. Наприклад, якщо кінцевою точкою є пряма лінія, то кут визначається напрямком кінцевої точки.

Окрім використання положення та кута нахилу контрольних точок, також можлива класифікація контрольних точок за типом та якістю. Перевагою цієї класифікації є те, що особливо важливі деталі достатньо висвітлені, щоб прискорити пошук.

Аномалії, спричинені подряпинами, потом, брудом тощо, відображаються як помилкові хвилинні позначки, а алгоритм розпізнає безглузді крапки та візерунки, такі як вилки пальців та кілька перпендикулярних ліній, що перетинаються (можливі подряпини або бруд). Тому більшість хвилинних позначок при цьому відкидаються.

Точність відповідності системи автентифікації залежить від стабільності біометричних даних, пов'язаних з особою в часі. Біометричні дані особи чутливі до змін, спричинених неналежною взаємодією з датчиками (наприклад, часткові відбитки пальців), зміною характеристик

датчиків (наприклад, оптичних або твердотільних датчиків відбитків пальців), зміною факторів навколишнього середовища (наприклад, слабкі відбитки пальців через посуху) та зміною самих біометричних характеристик з часом (наприклад, порізи/задирки відбитків пальців). Як наслідок, збережені шаблонні дані можуть суттєво відрізнятися від даних, отриманих під час автентифікації, що призводить до погіршення роботи біометричної системи (збільшення кількості хибних спрацьовувань).

Одним із способів вирішення проблеми наявності різних відбитків пальців однієї і тієї ж особи є зберігання декількох зразків одного і того ж відбитка пальця в базі даних зразків. Наприклад, можна зберігати кілька відбитків пальців, що належать до різних частин пальця, для обробки випадків, коли користувачі по-різному прикладають палець до датчика.

2.4.2 Відповідність

Автоматичне виявлення рукописів виявилося особливо складним для відбитків пальців низької якості, оскільки шум і недостатня контрастність можуть викликати скупчення пікселів, які виглядають як рукописи і маскують справжній рукопис. Успішне зіставлення вимагає ретельного вилучення особливостей відбитків пальців, пошуку шаблонів з потрібними характеристиками та надання можливості алгоритму зіставлення ефективно порівнювати деталі зображення та елементи шаблону.

Алгоритми, які не базуються на мінуціях

Ці алгоритми порівнюють базові шаблони відбитків пальців (дуги, криві та петлі) з раніше збереженими шаблонами та потенційними відбитками пальців. Це часто вимагає, щоб зображення були вирівняні в одній орієнтації. Для цього алгоритм знаходить центр зображення відбитка пальця та центрує його. Для алгоритмів, які не використовують малі літери, шаблон містить тип, розмір та орієнтацію візерунка на вирівняному зображенні відбитка пальця. Зображення відбитків пальців кандидата та шаблон порівнюються для визначення ступеня збігу.

2.4.3 Біометричні процесори

Виконання алгоритмів розпізнавання відбитків пальців вимагає цифрових обчислювальних потужностей та об'єму пам'яті. У додатках, оснащених власними високопродуктивними процесорами, таких як мобільні телефони, ці алгоритми можуть виконуватися на одному процесорі, що виступає в ролі головного процесора. Для інших застосувань, таких як дверні замки та зчитувачі карток, де продукт не має центрального процесора, що взаємодіє безпосередньо з датчиком відбитків пальців, потрібен спеціальний біометричний процесор як частина рішення.

Біометричні процесори - це цифрові мікросхеми для біометричної ідентифікації. Процесор виконує реєстрацію, ідентифікацію та верифікацію шляхом реалізації відповідних алгоритмів вилучення та зіставлення. Оскільки енергоспоживання і розмір мають вирішальне значення для багатьох застосувань, біометричні процесори повинні бути невеликими і енергоефективними. Потім біометричний процесор підключається до хоста продукту через стандартний інтерфейс, наприклад, послідовний порт, для отримання команд і виведення результатів.

3 РОЗРОБКА 3D МОДЕЛІ ДЛЯ ВІДБИТКІВ ПАЛЬЦІВ

3.1 Введення

В даний час в дактилоскопічній ідентифікації осіб переважає порівняння мініатюрних-мініатюрних розподілів, так званих локальних ознак. Це визначено в міжнародних стандартах [10]. Одним з факторів, що ускладнює досягнення високої точності співставлення, є те, що різні реалізації одного і того ж біометричного образу можуть викликати лінійні (афінні) спотворення в розподілі мікронерівностей. Тому викликом залишається вибір та розробка ефективних індексів порівняння, на які не впливають лінійні та нелінійні викривлення.

Розглянемо тепер нову метрику оцінки, засновану на переході від звичайного плоского розподілу локальних особливостей до тривимірного представлення 3D. Основною перевагою цього показника є незалежність від порушень порядку перерахування точок у біометричних шаблонах, визначених стандартом [10]. Як і евклідів показник, цей показник є стійким до лінійних зсувів та поворотів і, що більш важливо, до відмінностей у кількості характерних точок у реалізації шаблонів, що порівнюються. В даній роботі аналізується найпростіший варіант 3D метрики, коли для характеристики мініатюрних точок використовуються лише координати мініатюрних точок на площині .$\left(X,Y\right)_i$

3.2 Розробка та описання алгоритму

На рисунку 19 показано вплив спотворення шляхом порівняння двох розподілів різних реалізацій одного і того ж шаблону відбитків пальців. Реалізації базуються на відкритій базі даних [11]; у двох різних реалізаціях спостерігалися лінійні та нелінійні спотворення мініатюрних розподілів. Для гарантування незалежності міри подібності планарного розподілу Мануші від

афінних спотворень та відмінностей у кількості точок виявлення були введені 3D метрики. Домінуючий характер цих спотворень унеможливлює послідовну нумерацію розподілів мікронерівностей, отриманих з різних реалізацій зображення одного і того ж відбитка пальця. Це ускладнює використання звичайних евклідових метрик для кількісної оцінки близькості двох плоских точкових розподілів.

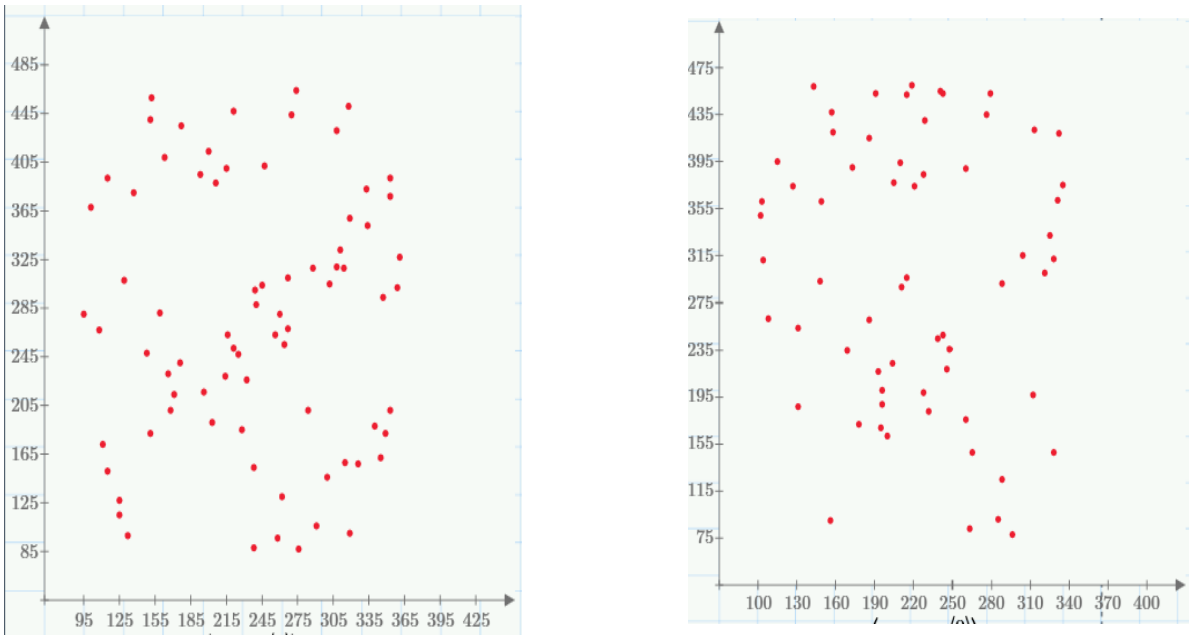


Рисунок 3.1 - Порівняння розподілів мінуцій для двох різних реалізацій відбитка

3D метрики надають більше можливостей для автентифікації, враховуючи не лише координати точки, але й якісні показники, такі як тип виявленої мінуції та кут прильоту. Цього можна досягти шляхом введення залежності параметрів і типів геометричних примітивів від числових властивостей відповідних маневрів.

Розглянемо та проілюструємо математичний та фізичний зміст 3D метрики на простому прикладі переходу до тривимірних поверхонь з використанням лише одного геометричного примітиву - конуса постійної висоти, побудованого на центрі кожної характерної точки.

Нижче наведено короткий огляд алгоритму перетворення та розрахунок показників FRR (частота помилкових відмов), FAR (частота помилкових прийняттів) та EER (частота однакових помилок). В якості геометричного примітиву для перетворення плоского розподілу точок обрано простий симетричний конус. Його основою є коло радіусом r , а висота дорівнює h .

Експериментально встановлено, що найвища середня точність автентифікації на основі 3D метрики досягається на сайті $r = 75$. Параметр h не має суттєвого впливу на результати і його зміна лише зміщує діапазон взаємних відстаней. Тому для простоти обрано $h = 1$. Параметричне рівняння позитивно визначеного конуса на площині має вигляд

$$v(x, y, a, b) = \begin{cases} h - \frac{1}{r}\sqrt{(x-a)^2 + (y-b)^2} & if \ \ \frac{1}{r}\sqrt{(x-a)^2 + (y-b)^2} \le h; \\ 0 \quad otherwize. \end{cases} \tag{3.1}$$

де x, y - поточні координати; a, b - координати центру підстави, тобто координати обраної Мінуцій, над якою відновлюється конус. Вид використовуваного графічного примітиву, що визначається з (1), показаний на рис. 20.

Чисельна оцінка абсолютної величини обсягу, який взятий під поверхнею геометричного примітиву, показаного на рис. 20, становить

$$V0 = \frac{1}{Nv \cdot Ng} \sum_{i=0}^{Nv-1} \sum_{j=0}^{Ng-1} \left| S0(i, j) \right| \approx 0.025. \tag{3.2}$$

Оцінка схожості/відмінності двох мінуцій розподілів 3D метрик за величиною, пропорційною певному об'єму. Слід зазначити, що практична відносна симетрія 3D метрики відносно афінних спотворень проявляється в тому, що

- Обертання одного зображення в протилежному напрямку під тим же кутом до іншого зображення дає ті ж самі взаємні оцінки відстаней.

- Таку ж взаємну відстань можна оцінити при лінійному переміщенні одного зображення на певну відстань до іншого зображення.

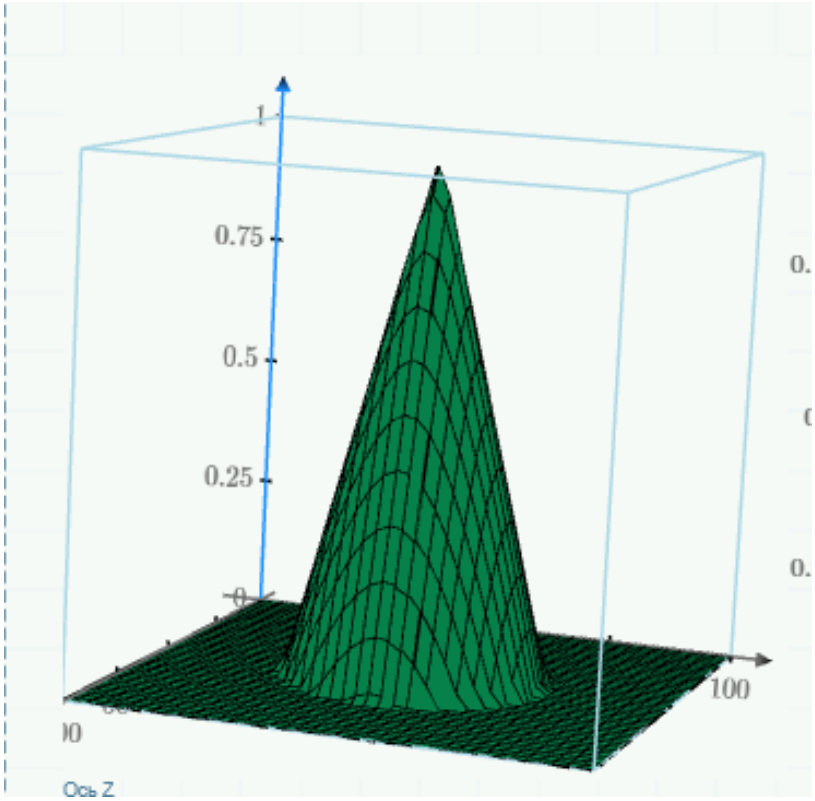


Рисунок 3.2 - Геометричний примітив 3D метрики

При цьому немає необхідності перераховувати переміщені точки по порядку (як у випадку з евклідовою метрикою). Про низьку чутливість 3D метрики до втрати реальних точок та додавання хибних точок свідчать дуже малі зміни оцінок взаємних відстаней, які наведені нижче $\left|(p+q)\cdot V0\right|$, . Де p та q - кількість видалених та доданих балів. Хороші властивості метрики були обрані в результаті обертальної симетрії геометричних примітивів.

Параметричне рівняння поверхні, що відповідає біометричному шаблону m -го пальця n -го скану людини, має вигляд простої алгебраїчної суми рівнянь конусів, відновлених над кожною мініатюрою, присутньою в шаблоні.

$$S0(x,y,k,m,n)=\sum_{i=0}^{N-1} v\left[x,y,\left(\left((F_k)_m\right)_n^{\langle 1\rangle}\right)_i,\left(\left((F_k)_m\right)_n^{\langle 2\rangle}\right)_i\right], \qquad (3.3)$$

де N - число мінуцій в шаблоні

$\left(\left(\left(F_k\right)_m\right)_n^{\langle 1\rangle}\right)_i$, $\left(\left(\left(F_k\right)_m\right)_n^{\langle 2\rangle}\right)_i$ - координати X і Y, відповідно, для i-тої мінуції

Абсолютне значення різниці об'ємів використовується як показник взаємної віддаленості двох 3D зображень біометричних шаблонів $(k1, m1, n1)$ та $(k2, m2, n2)$. Для розрахунку цього показника спочатку визначимо параметричне рівняння поверхні Δk , яке отримуємо шляхом алгебраїчного віднімання (за абсолютною величиною) рівняння одного шаблону від рівняння іншого.

$$\Delta k\left(x, y, k1, m1, n1, k2, m2, n2\right) = \left|S\left(x, y, k1, m1, n1\right) - S\left(x, y, k2, m2, n2\right)\right| \qquad (3.4)$$

Тоді властивість взаємної відстані тривимірних метрик має значення

$$V\_diff\left(k1, m1, n1, k2, m2, n2\right) = \frac{1}{M^2}\sum_{i\in M}\sum_{j\in M}\Delta k\left(i\cdot\Delta i,\ j\cdot\Delta j, k1, m1, n1, k2, m2, n2\right). \qquad (3.5)$$

Достатньо знайти значення Δk лише в 100 точках на площині зображення (10 точок по осі (X, Y)). Параметричне рівняння диференціальної поверхні пари поверхонь, зображеної на рисунку 21, має вигляд

$$\Delta k\left(x, y, 0, 0, 0, 0, 0, 5\right) = \left|S\left(x, y, 0, 0, 0\right) - S\left(x, y, 0, 0, 5\right)\right|$$

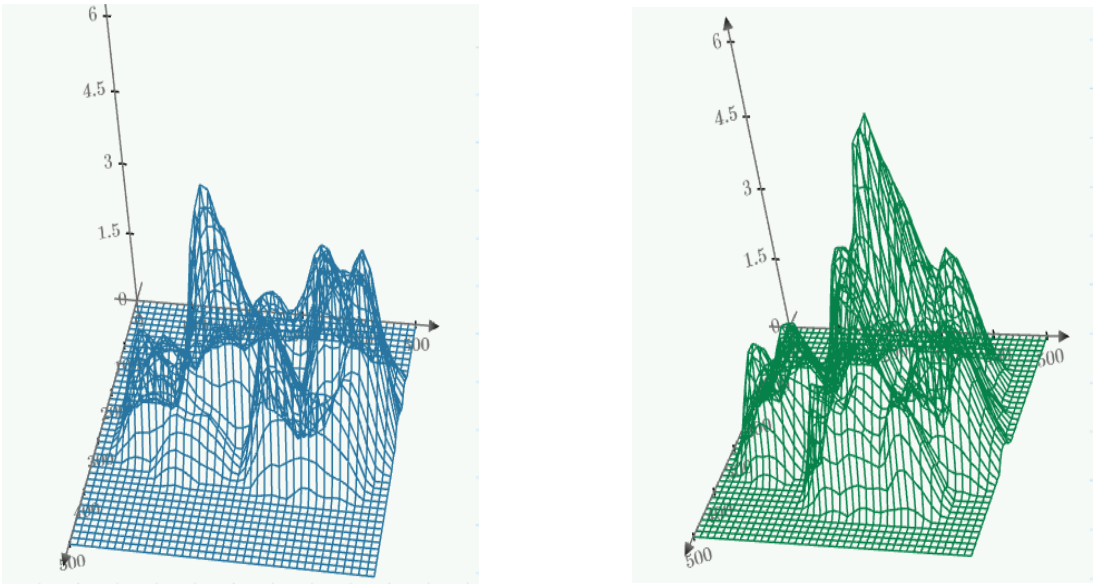


Рисунок 3.3 - 3D уявлення біометричних шаблонів для двох реалізацій одного і того ж об'єкта аналізованої бази: $(k=0, m=0, n=0)$ і $(k=0, m=0, n=5)$.

а уявлення цієї різницевої поверхні, буде мати форму, показану на рис. 3.4.

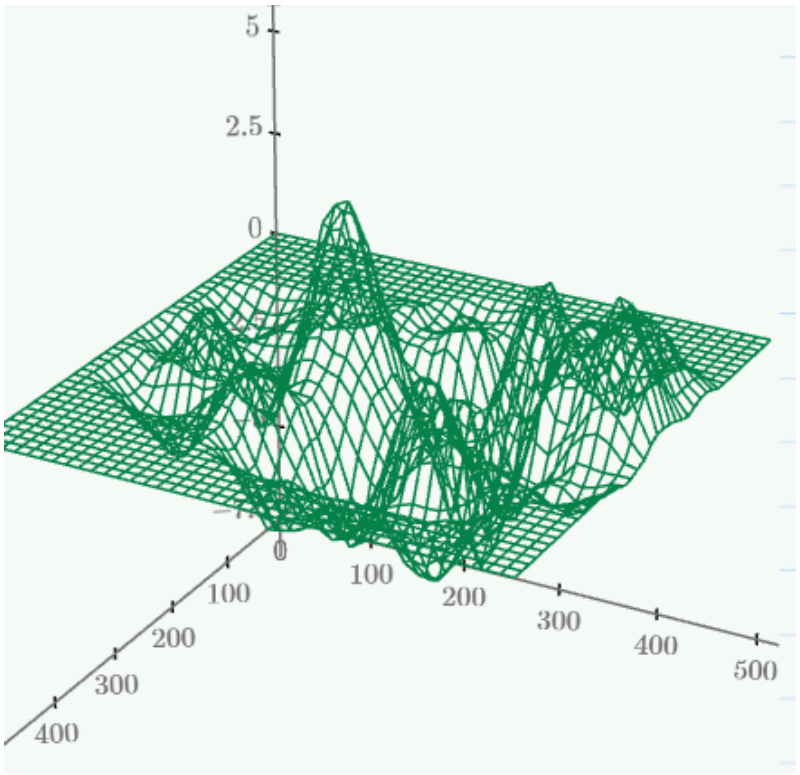


Рисунок 3.4 - 3D представлення поверхні відмінностей біометричного шаблону двох реалізацій, що аналізують один і той самий об'єкт бази даних: $(k=0, m=0, n=0)$ та $(k=0, m=0, n=5)$

Використання формули (5) дає наступну величину разностного обсягу, укладеного під показаної на рис. 22 поверхнею

$$V\_diff\,(0,0,0,0,0,5) = \frac{1}{100}\sum_{i=0}^{9}\sum_{j=0}^{9}\Delta k\,(i\cdot 48,\ j\cdot 50,0,0,0,0,0,5) \approx 0.3 \qquad (3.6)$$

Для порівняння, поверхні відмінностей, отримані при порівнянні різних дактилоскопічних шаблонів, наведені на рисунку 23. Взаємні відстані між шаблонами, що належать різним особам, розраховуються у 3D метриці. Цей

приклад добре ілюструє об'єктивність 3D метрики в оцінці схожості біометричних шаблонів.

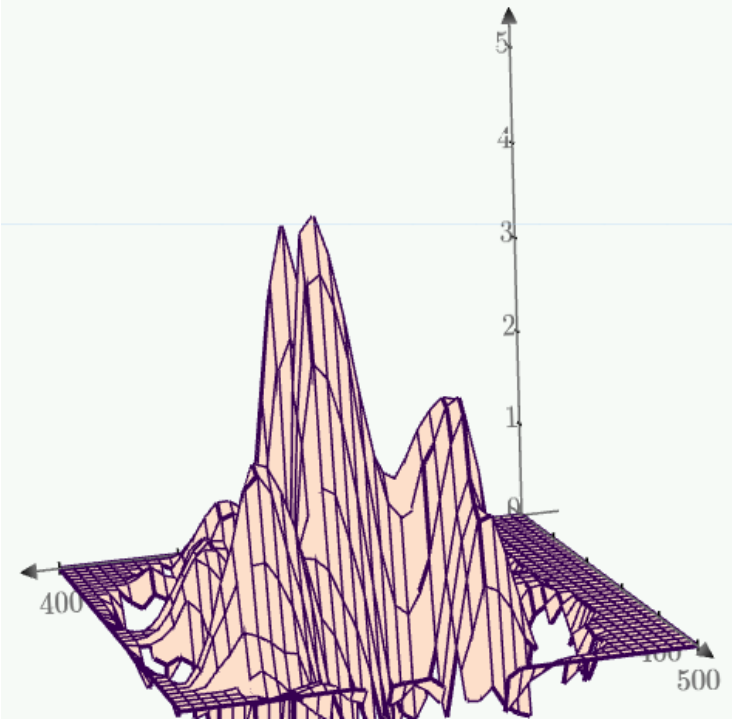


Рисунок 3.5 - 3D представлення диференціальних поверхонь біометричних шаблонів двох різних об'єктів в аналізованій базі даних: $(k=0, m=0, n=0)$ та $(k=5, m=0, n=0)$

3.3 Тестування

Для перевірки точності процесу автентифікації було обрано метод вичерпної перехресної перевірки, який вимагає найбільшої кількості розрахунків і є найбільш витратним, але при цьому забезпечує найбільш надійну "жорстку" межу показників якості. На рис. 24 наведено результати статистичних тестів запропонованих 3D метрик, виконаних на базі даних відбитків пальців [11]. Індикатор EER , який використовував просту 3D метрику, що враховувала лише координати мініатюр і використовував один геометричний примітив, був.

$$EER \approx 19\%$$

Таким чином, можна констатувати наявність досить високої стійкості метрики до дії лінійних спотворень; точність 3D метрики може бути суттєво

підвищена за рахунок використання різних типів геометричних примітивів та додаткових властивостей маневру.

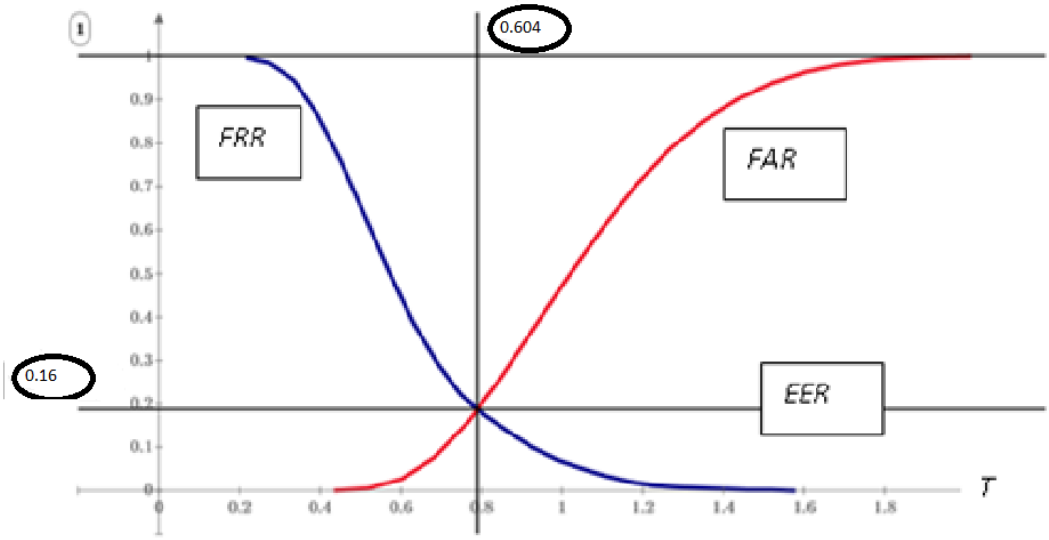


Рисунок 3.6 - Функції FRR, FAR і рівень EER для зіставлень в 3D метриці.

ВИСНОВОК

Ця робота присвячена системам біометричної ідентифікації за відбитками пальців. Існує ряд дуже важливих питань, пов'язаних з системами ідентифікації за відбитками пальців, включаючи шифрування, безпеку шаблонів відбитків пальців, виявлення помилкових відбитків пальців і питання конфіденційності. Ці питання, які потребують системного вирішення при розгортанні надійних систем дактилоскопічної ідентифікації у великих масштабах, виходять за рамки даного курсу.

Надійність автоматизованих дактилоскопічних систем значною мірою залежить від точності процесу вилучення відбитків пальців. Існує низка факторів, які можуть перешкоджати правильному розміщенню контрольних пунктів. Найсерйозніші з них - низька якість читання, зникнення, додавання підробок, обертання та масштабування.

Існує низка подальших удосконалень, які можуть бути зроблені з точки зору ефективності та точності шляхом модернізації обладнання для отримання зображень та технології зчитування відбитків пальців.

Однак, коли справа доходить до співставлення відбитків пальців, все ще залишається багато проблем. Наприклад, майже всі сучасні засоби дактилоскопічної ідентифікації можуть бути підроблені з використанням підроблених пальців (наприклад, щільно прилягаючих латексних рукавичок, які створюють враження чужих пальців, відбитків пальців).

Виявлення життєздатності відбитків пальців є складною проблемою. Індикатори виживання або ідентифікатори виживання часто є більш поведінковими характеристиками і мають тенденцію до

Це має сенс, але зчитувачі відбитків пальців і системи автентифікації повинні прагнути до того, щоб зробити підробку відбитків пальців все більш складною, включивши в себе функції захисту від підробки.

Існуючі комбіновані системи аутентифікації (мінути і банки фільтрів) в апаратному і програмному виконанні поки що не здатні впоратися з відбитками пальців дуже низької якості і великими нелінійними спотвореннями. За оцінками, 4% населення, включаючи людей похилого віку, жінок азіатського походження та працівників фізичної праці, не мають якісних відбитків пальців і мають проблеми з системою зіставлення.

Комплексний аналіз переваг і недоліків відбитків пальців як біометрії показує, що найбільш поширена дактилоскопічна технологія досягла рівня продуктивності (рівень помилок, час), достатнього для різноманітних споживчих додатків, а системи зчитування відбитків пальців вже є повсюдними. Як наслідок, вартість пристроїв дактилоскопічної ідентифікації продовжує знижуватися.

Наприкінці дипломного проекту було розроблено алгоритм побудови конуса на вершині кожної мініатюри з використанням математичної тривимірної метрологічної моделі для верифікації відбитка пальця. Коли всі конуси побудовані, вони виглядають як гора. Ця гора є унікальним відбитком пальця в моєму алгоритмі і має бути унікальною для кожної людини. Перевага мого алгоритму в тому, що він миттєво захищений від повороту пальця. Цей алгоритм є слабким сам по собі, але в поєднанні з іншими перевірками він може бути конкурентоспроможним на ринку.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chellappa R., Wilson C. & Sirohey S. Human and machine recognition of faces: a survey. 1995. 36 p.
2. Khushk K., Iqbal A., An Overview of Leading Biometrics Technologies Used for Human Identity. In Engineering Sciences and Technology. Karlskorna, 2005. 79 p.
3. Stamp M., Information security: principles and practice, John Wiley & Sons, Inc. 2006. 413 p.
4. Liu S., Silverman M., A practical guide to biometric security technology. 2001. 315 p.
5. O'Gorman L., Comparing passwords, tokens, and biometrics for user authentication. 2003. 264 p.
6. Yun Y.W., The ‘123’ of Biometric Technology. Biometrics Working Group of Security & Privacy Standards Technical Committee. 2002.14 p.
7. Allan R., Biometrics Wields a Double-Edged Sword. Electronic Design. 2005. 329 p.
8. Chandra A., Calderon, T., Challenges and constraints to the diffusion of biometrics in information systems. 2005. 317 p.
9. Разработка математической модели верификационной метрики, устойчивой к афинным искажениям шаблонов локальных признаков отпечатков пальцев / С.Г.Рассомахін та ін. 2010. 7 с.
10. ISO/IEC 19794-2:2005 Information technology — Biometric data interchange formats – Part 2: Finger minutiae data.
11. Fingerprint Verification Competition FVC 2000-2004. URL: http://bias.csr.unibo.it/fvc2004/databases.asp (дата звернення: 18.05. 2021).

ДОДАТОК А

КОД ПРОЕКТУ РЕАЛІЗАЦІЇ МАТЕМАТИЧНОЇ МОДЕЛІ 3D-МЕТРИКИ ДЛЯ ВЕРИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ

$$T := \text{READFILE}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash 0\_0.txt”}, \text{“delimited”})$$

$$T1 := \text{READFILE}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash 0\_1.txt”}, \text{“delimited”})$$

$$ii := 0 \qquad jj := 0$$

$$T3_{0,0} := \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash ”}, \text{num2str}(ii), \text{“\_”}, \text{num2str}(jj), \text{“.txt”}), \text{“delimited”})$$

$$T3_{0,1} := \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash ”}, \text{num2str}(ii), \text{“\_”}, \text{num2str}(jj+1), \text{“.txt”}), \text{“delimited”})$$

$$T3_{1,1} := \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash ”}, \text{num2str}(ii+1), \text{“\_”}, \text{num2str}(jj+1), \text{“.txt”}), \text{“delimited”})$$

$$T3_{2,2} := \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash ”}, \text{num2str}(ii+2), \text{“\_”}, \text{num2str}(jj+2), \text{“.txt”}), \text{“delimited”})$$

$$T4 := \left\| \begin{array}{l} \text{for } ii \in 0..50 \\ \quad N_{ii} \leftarrow ii \\ \text{return } N \end{array} \right. \qquad T5 := \left\| \begin{array}{l} \text{for } ii \in 0..50 \\ \quad \text{for } jj \in 0..7 \\ \quad\quad N_{ii,jj} \leftarrow ii \\ \text{return } N \end{array} \right.$$

$$T4 = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \\ \vdots \end{bmatrix} \qquad T5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\ 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 \\ 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ & & & & & & & \vdots \end{bmatrix}$$

$$T3 := \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash”}, \text{num2str}(ii), \text{“\_”}, \text{num2str}(jj), \text{“.txt”}), \text{“delimited”})$$

$$T6 := \left\| \begin{array}{l} \text{for } ii \in 0..50 \\ \quad \left\| \begin{array}{l} \text{for } jj \in 0..7 \\ \quad \left\| T3_{ii,jj} \leftarrow \text{READFILE}(\text{concat}(\text{“Templ\_qxy\_TXT\_CMS\textbackslash”}, \text{num2str}(ii), \text{“\_”}, \text{num2str}(jj), \text{“.txt”}), \text{“delimited”}) \right. \end{array} \right. \\ \text{return } T3 \end{array} \right.$$

$$T6 = \begin{bmatrix} [76\times3] & [63\times3] & [66\times3] & [79\times3] & [84\times3] & [73\times3] & [97\times3] & [85\times3] \\ [68\times3] & [73\times3] & [61\times3] & [58\times3] & [65\times3] & [74\times3] & [67\times3] & [61\times3] \\ [75\times3] & [79\times3] & [71\times3] & [76\times3] & [73\times3] & [73\times3] & [72\times3] & [77\times3] \\ [68\times3] & [105\times3] & [89\times3] & [99\times3] & [87\times3] & [89\times3] & [94\times3] & [99\times3] \\ [65\times3] & [66\times3] & [70\times3] & [64\times3] & [55\times3] & [61\times3] & [62\times3] & [65\times3] \\ [64\times3] & [88\times3] & [71\times3] & [62\times3] & [79\times3] & [65\times3] & [60\times3] & [84\times3] \\ [60\times3] & [60\times3] & [61\times3] & [63\times3] & [64\times3] & [75\times3] & [71\times3] & [61\times3] \\ [72\times3] & [74\times3] & [71\times3] & [72\times3] & [87\times3] & [80\times3] & [94\times3] & [83\times3] \\ [64\times3] & [71\times3] & [70\times3] & [75\times3] & [78\times3] & [80\times3] & [96\times3] & [83\times3] \\ [99\times3] & [85\times3] & [96\times3] & [99\times3] & [102\times3] & [78\times3] & [93\times3] & [73\times3] \\ [51\times3] & [58\times3] & [67\times3] & [59\times3] & [56\times3] & [54\times3] & [65\times3] & [52\times3] \\ [72\times3] & [75\times3] & [75\times3] & [77\times3] & [76\times3] & [78\times3] & [82\times3] & [72\times3] \\ & & & & & & & \vdots \end{bmatrix}$$

Полная матрица базы

$$T7 := \left\| \begin{array}{l} \text{for } i \in 0..\text{last}\left\langle T6^{\langle 0 \rangle} \right\rangle \\ \quad \left\| \begin{array}{l} \text{for } j \in 0..\text{last}\left(\left(T6^{\overset{\frown}{0}}\right)^{\mathrm{T}}\right) \\ \quad \left\| t7_{i,j} \leftarrow \text{submatrix}\left(T6_{i,j}, 0, \text{last}\left(T6_{i,j}^{\langle 0 \rangle}\right), 1, 2\right) \right. \end{array} \right. \\ t7 \end{array} \right.$$

Матрица базы, содержащая только X,Y

$$h := 1$$

$$v(x,y,a,b) := \text{if } \frac{1}{r} \cdot \sqrt{(x-a)^2 + (y-b)^2} \le h \left\| \begin{array}{l} h - \frac{1}{r} \cdot \sqrt{(x-a)^2 + (y-b)^2} \\ \text{else} \\ 0 \end{array} \right.$$

$$T = \begin{bmatrix} 0.384 & 95 & 280 \\ 0.576 & 101 & 368 \\ 0.384 & 108 & 267 \\ 0.576 & 111 & 173 \\ 0.785 & 115 & 151 \\ 0.785 & 115 & 392 \\ 0.785 & 125 & 115 \\ 0.785 & 125 & 127 \\ 0.384 & 129 & 308 \\ 0.977 & 132 & 98 \\ 0.576 & 137 & 380 \\ 3.526 & 148 & 248 \\ 0.785 & 151 & 182 \\ 0.977 & 151 & 440 \\ 1.169 & 152 & 458 \\ 3.526 & 159 & 281 \\ 0.785 & 163 & 409 \\ & & \vdots \end{bmatrix} \qquad i := 0..400 \qquad T1 = \begin{bmatrix} 0.785 & 102 & 349 \\ 0.977 & 103 & 361 \\ 0.576 & 104 & 311 \\ 0.384 & 108 & 262 \\ 0.977 & 115 & 395 \\ 0.977 & 127 & 374 \\ 0.576 & 131 & 187 \\ 0.384 & 131 & 254 \\ 1.169 & 143 & 459 \\ 0.384 & 148 & 293 \\ 0.785 & 149 & 361 \\ 0.977 & 156 & 90 \\ 1.169 & 157 & 437 \\ 0.977 & 158 & 420 \\ 3.526 & 169 & 235 \\ 0.785 & 173 & 390 \\ 0.785 & 178 & 172 \\ & & \vdots \end{bmatrix}$$

$Txy := \text{submatrix}\left(T, 0, \text{last}\left(T^{(0)}\right), 1, 2\right)$

$Txy =$

95	280
101	368
108	267
111	173
115	151
115	392
125	115
125	127
129	308
132	98
137	380
148	248
151	182
151	440
152	458
159	281
163	409
166	231
⋮	

$Txy1 := \text{submatrix}\left(T1, 0, \text{last}\left(T1^{(0)}\right), 1, 2\right)$

$Txy1 =$

102	349
103	361
104	311
108	262
115	395
127	374
131	187
131	254
143	459
148	293
149	361
156	90
157	437
158	420
169	235
173	390
178	172
186	261
⋮	

$$V00(x,y) := 1 \sum_{i=0}^{\text{last}\left(\left(T6_{k,n}\right)^{(1)}\right)} v\left(x, y, \left(T6_{k,n}\right)_{i,1}, \left(T6_{k,n}\right)_{i,2}\right)$$

$$V01(x,y) := 1 \sum_{i=0}^{\text{last}\left(\left(T6_{k+1,n}\right)^{(1)}\right)} v\left(x, y, \left(T6_{k+1,n}\right)_{i,1}, \left(T6_{k+1,n}\right)_{i,2}\right)$$

$k \equiv 0 \qquad n \equiv 4$

$$Vdif := \frac{1}{Ns^2} \cdot \sum_{j=0}^{Ns-1} \sum_{i=0}^{Ns-1} \left| \left(V00\left(\frac{MaxX}{Ns} \cdot j, \frac{MaxY}{Ns} \cdot i\right) - V01\left(\frac{MaxX}{Ns} \cdot j, \frac{MaxY}{Ns} \cdot i\right) \right) \right|$$

$Vdif = 0.572$

$h := 1$

$$v(x,y,a,b) := \begin{cases} \text{if } \frac{1}{r} \cdot \sqrt{(x-a)^2 + (y-b)^2} \le h \\ \quad \left\| h - \frac{1}{r} \cdot \sqrt{(x-a)^2 + (y-b)^2} \right. \\ \text{else} \\ \quad \| 0 \end{cases}$$

$$S(x,y,A) := \sum_{i=0}^{\text{last}(A^{(1)})} v\left(x,y,A_{i,0},A_{i,1}\right)$$ построение поверхности для шаблона A

$$V0(x,y) := 1 \sum_{i=0}^{\text{last}(Txy^{(0)})} v\left(x,y,Txy_{i,0},Txy_{i,1}\right)$$

$$V1(x,y) := 1 \sum_{i=0}^{\text{last}(Txy1^{(0)})} v\left(x,y,Txy1_{i,0},Txy1_{i,1}\right)$$

$Ns \equiv 10$ $MaxX \equiv 400$ $MaxY \equiv 500$ $r \equiv 50$

Матрица взаимных расстояний для 0 объекта (Genuine)

$$M\_Dist\_G0 := \left\| \begin{array}{l} \text{for } i \in 0..6 \\ \quad \text{for } j \in i+1..7 \\ \quad\quad m\_d_{i,j} \leftarrow \frac{1}{Ns^2} \cdot \sum_{k0=0}^{Ns-1} \sum_{m0=0}^{Ns-1} \left| \left(S\left(\frac{MaxX}{Ns} \cdot k0, \frac{MaxY}{Ns} \cdot m0, T7_{0,i}\right) - S\left(\frac{MaxX}{Ns} \cdot k0, \frac{MaxY}{Ns} \cdot m0, T7_{0,j}\right)\right)\right| \\ m\_d \end{array} \right\|$$

Матрица взаимных расстояний для всех 51 объектов (Genuine)

$$M\_Dist\_G := \left\| \begin{array}{l} \text{for } i0 \in 0..\text{last}\left(T7^{(0)}\right) \\ \quad mm_{i0} \leftarrow \left\| \begin{array}{l} \text{for } i \in 0..6 \\ \quad \text{for } j \in i+1..7 \\ \quad\quad m\_d_{i,j} \leftarrow \frac{1}{Ns^2} \cdot \sum_{k0=0}^{Ns-1} \sum_{m0=0}^{Ns-1} \left| \left(S\left(\frac{MaxX}{Ns} \cdot k0, \frac{MaxY}{Ns} \cdot m0, T7_{i0,i}\right) - S\left(\frac{MaxX}{Ns} \cdot k0, \frac{MaxY}{Ns} \cdot m0, T7_{i0,j}\right)\right)\right| \\ m\_d \end{array} \right. \\ mm \end{array} \right\|$$

$$V\_dist\_G := \left\| \begin{array}{l} Ct \leftarrow 0 \\ \text{for } i \in 0..\text{last}\left(T7^{(0)}\right) \\ \quad \text{for } i0 \in 0..6 \\ \quad\quad \text{for } j0 \in i0+1..7 \\ \quad\quad\quad v_{Ct} \leftarrow \left(M\_Dist\_G_i\right)_{i0,j0} \\ \quad\quad\quad Ct \leftarrow Ct+1 \\ v \end{array} \right\|$$

$$HistG := \text{histogram}\left(20, V\_dist\_G\right)$$

$$i3 := 0..\text{last}\left(HistG^{(0)}\right)$$

$$\text{mean}\left(V\_dist\_G\right) = 0.604$$

$$\text{stdev}\left(V\_dist\_G\right) = 0.16$$

$$\frac{1}{51 \cdot 28} \cdot \sum_{i=0}^{\text{last}(HistG^{(0)})} \left(HistG^{(1)}\right)_i = 1$$

$$Vdif(S0,S1) := \frac{1}{Ns^2} \cdot \sum_{j=0}^{Ns-1} \sum_{i=0}^{Ns-1} \left| \left(V0\left(\frac{MaxX}{Ns}\cdot j, \frac{MaxY}{Ns}\cdot i\right) - V1\left(\frac{MaxX}{Ns}\cdot j, \frac{MaxY}{Ns}\cdot i\right)\right)\right|$$

$$M\_Dist\_I0 := \left\| \begin{array}{l} \text{for } i \in 0..7 \\ \quad \text{for } j \in 0..7 \\ \quad\quad m\_d_{i,j} \leftarrow \frac{1}{Ns^2} \cdot \sum_{k0=0}^{Ns-1} \sum_{m0=0}^{Ns-1} \left| \left(S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{0,i}\right) - S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{1,j}\right)\right)\right| \\ m\_d \end{array} \right\|$$

$$M\_Dist\_I0\_All := \left\| \begin{array}{l} \text{for } l \in 1..\text{last}\left(T7^{\langle 0\rangle}\right) \\ \quad m\_d\_a_l \leftarrow \left\| \begin{array}{l} \text{for } i \in 0..7 \\ \quad \text{for } j \in 0..7 \\ \quad\quad m\_d_{i,j} \leftarrow \frac{1}{Ns^2} \cdot \sum_{k0=0}^{Ns-1} \sum_{m0=0}^{Ns-1} \left| \left(S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{0,i}\right) - S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{l,j}\right)\right)\right| \\ m\_d \end{array} \right. \\ m\_d\_a \end{array} \right\|$$

$$M\_Dist\_I := \left\| \begin{array}{l} \text{for } l1 \in 0..49 \\ \quad m\_d\_i_{l1} \leftarrow \left\| \begin{array}{l} \text{for } l \in 1..\text{last}\left(T7^{\langle 0\rangle}\right) \\ \quad m\_d\_a_l \leftarrow \left\| \begin{array}{l} \text{for } i \in 0..7 \\ \quad \text{for } j \in 0..7 \\ \quad\quad m\_d_{i,j} \leftarrow \frac{1}{Ns^2} \cdot \sum_{k0=0}^{Ns-1} \sum_{m0=0}^{Ns-1} \left| \left(S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{l1,i}\right) - S\left(\frac{MaxX}{Ns}\cdot k0, \frac{MaxY}{Ns}\cdot m0, T7_{l,j}\right)\right)\right| \\ m\_d \end{array} \right. \\ m\_d\_a \end{array} \right. \\ m\_d\_i \end{array} \right\|$$