МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2020 р.

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«Магістр»

Тема: Система мультиекземплярної біометричної аутентифікації

Автор: А.В. Бахмач

Науковий керівник: к.т.н., доц. А.Б. Єлізаров

Нормоконтролер: к.т.н., доц. А.Б. Єлізаров

Київ 2020

ВСТУП

На сьогоднішній день інформаційні технології проникли майже в усі сфери нашого життя, тому проблема безпеки доступу до інформаційних систем і приватної інформації стала вкрай актуальною. Класична аутентифікація суб'єкта залежить від паролів і ключів, які можуть бути легко втрачені або забуті. Також вона не гарантує, що паролем користується саме той суб'єкт, якому надано доступ. Ця проблема може бути вирішена шляхом використання біометричної аутентифікації, тобто аутентифікації, яка перевіряє особу суб'єкта на основі його фізіологічних або поведінкових характеристик, таких як відбитки пальців, геометрія обличчя, голос тощо.

Тенденції розвитку біометрії й засновані на її принципах системи стали ефективним засобом убезпечення всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі та поліпшення іхньої ефективності є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектора, індустріальних і комерційних структур, так і для окремих громадян.

Актуальність роботи

Більша частина досліджень в області біометрії спрямована на збільшення точності й ефективності таких систем. Найчастіше для підвищення якості прийняття рішення застосовуються мультимодальні біометричні системи. Такі системи використовують більше однієї біометричної характеристики для розрахунку оцінки схожості. Такі системи дозволяють використовувати більшу кількість факторів для прийняття рішення. При даному підході через ускладнення системи класична бінарна логіка і порівняння з граничним значенням не дають

потрібного результату. Тому використовують нечітку логіку, так як даний підхід забезпечує меншу втрату інформації при роботі системи. Також вона дає можливість тонкого й детального налаштування системи за рахунок зміни параметрів нечіткого виводу. Це дозволяє змінювати пріоритет того чи іншого фактору, що впливає на рішення.

Тому актуальним є розробити метод навчання систем мультиекземплярної біометричної аутентифікації на основі правил нечіткої логіки, побудувати мультимодальну біометричну систему з підсистемою прийняття рішень на основі правил нечіткої логіки та проаналізувати, які переваги має дана система над іншими.

Мета і завдання дослідження

Метою роботи є підвищення ефективності систем біометричної аутентифікації, за рахунок розробки методу біометричної аутентифікації для розпізнавання відбитків пальців, побудови підсистеми прийняття рішень, заснованої на методах та правилах нечіткої логіки, дослідження якості даного методу в порівнянні з іншими стратегіями в даній області.

Завданням даного дослідження є аналіз предметної область систем розпізнавання відбитків пальців, а також основних принципів і понять нечіткої логіки, розробка методу навчання, створення прототипу мультиекземплярної системи для розпізнавання відбитків пальців, створення підсистеми прийняття рішень на основі правил нечіткої логіки та порівняння результатів розпізнавання з альтернативними стратегіями прийняття рішень.

Об’єкт дослідження

Аутентифікація за біометричними характеристиками

Предмет дослідження

Метод навчання системи мультиекземплярної біометричної аутентифікації для розпізнання відбитків пальців на основі правил нечіткої логіки.

Методи дослідження

У якості методів дослідження був застосований теоретичний підхід до аналізу біометричних методів та систем аутентифікації, а також емпіричний підхід до тестування побудованої системи.

Наукова новизна одержаних результатів

Наукова новизна даної дисертації полягає у розробці нового методу прийняття рішень, який відрізняється використанням правил нечіткої логіки, що дозволяє підвищити ефективність мультимодальних біометричних систем.

1 БІОМЕТРИЧНІ МЕТОДИ АУТЕНТИФІКАЦІЇ

1.1 Біометрична аутентифікація

Аутентифікація (з грец. *αυθεντικός*; реальний або істинний) — процедура встановлення належності суб’єктові інформації в системі пред'явленого ним ідентифікатора [1].

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності і вартості впровадження.

Виділяють 3 фактори аутентифікації:

- **Щось, що ми знаємо – пароль.** Це таємні відомості, якими повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або особистий ідентифікаційний номер (PIN). Парольний механізм може бути досить легко втілений і має низьку вартість. Однак має суттєві недоліки: зберегти пароль у таємниці часто буває складно, зловмисники постійно придумують нові способи крадіжки, злому і підбору пароля, такі як бандитський криптоаналіз або метод грубої сили. Це робить парольний механізм слабо захищеним [1].
- **Щось, що ми маємо – пристрій аутентифікації.** Важливим є те, що суб'єкт володіє якимось неповторним предметом. Це може бути особиста печатка, ключ від замка, для комп'ютера – це файл даних, що містять певну характеристику. Характеристика часто вбудовується в спеціальний електронний пристрій аутентифікації, наприклад, пластикова карта, смарт-карта. Для зловмисника роздобути такий

пристрій стає більш складною задачею, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це робить даний метод більш захищеним, ніж парольний механізм, проте вартість такої системи більш висока [1].

- **Щось, що є частиною нас – біометрія.** Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або особливість ока. З точки зору суб'єкта, даний спосіб є найбільш простим: не треба ні запам'ятовувати пароль, ні переносити з собою пристрій аутентифікації. Однак біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого суб’єкта, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить велика. Але, не дивлячись на свої недоліки, біометрія залишається найнадійнішим та досить перспективним фактором [1].

У даній роботі буде побудована система, яка заснована на третьому факторі аутентифікації, а саме на біометрії. Тому розглянемо даний фактор більш детально.

Біометрія — це сукупність автоматизованих методів і засобів аутентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці [2]. Прикладами фізіологічних характеристик є відбитки пальців, форма руки, характеристика обличчя, райдужна оболонка ока тощо. До поведінкових характеристик відносяться особливості або характерні риси, або придбані, або що з'явилися згодом, тобто динаміка підпису, ідентифікація голосу, динаміка натискання на клавіші тощо. Біометрія – унікальна, вимірювана характеристика людини для автоматичної ідентифікації або верифікації. Термін «автоматично» означає, що біометричні системи повинні ідентифікувати або верифікувати людину швидко і автоматично, в режимі реального часу. Ідентифікація за допомогою біометричних систем передбачає порівняння первинного біометричного зразка з поновленими біометричними даними.

У біометрії існує відмінність між термінами **ідентифікація** та **верифікація**. Якщо говорити про ідентифікацію, то система намагається знайти, кому належить даний зразок, порівнюючи зразок з базою даних для того, щоб знайти збіг (також цей процес називають порівняння “одного до багатьох”).

Верифікація – це порівняння, при якому біометрична система намагається верифікувати особистість людини. У цьому випадку, новий біометричний зразок порівнюється з раніше збереженим зразком. Порівнюючи ці два зразка, система підтверджує, що ця людина дійсно та, за кого вона себе видає. У процесі ідентифікації система порівнює один зразок з багатьма, тоді як процес аутентифікації або верифікації порівнює “один з одним”. Ідентифікаційна система запитує: «Ви хто?». Верифікаційна система запитує «Ви дійсно той, за кого себе видаєте?».

Всі системи біометричної аутентифікації виконують дві основні функції [2]:

- *реєстрацію* – за декількома вимірюваннями зі зчитувального біометричного пристрою формується цифрове представлення (шаблон або модель) біометричної характеристики (в залежності від методу: відбиток пальця, рисунок райдужної оболонки ока тощо), відповідної реєстрованої людини;
- *розпізнавання* – один або декілька вимірів біометричної характеристики зчитуючого пристрою перетвориться на придатну для використання цифрову форму і потім порівнюється з:
    а) єдиним шаблоном, що відповідає людині, яка перевіряється. Шаблон обирається за попереднім запроваджуваним номером або кодом. Результати порівняння повертаються додатком — така процедура називається **верифікацією** або **порівнянням «один до одного»**. Результатом порівняння зазвичай є число-ймовірність того, що порівнювані шаблони належать одній особі. Потім, з використанням будь-якого математичного критерію, приймається рішення про ідентичність шаблонів;

b) з усіма зареєстрованими шаблонами (без попереднього вибору шаблону і введення номера або коду). Як результат, повертається список декількох найбільш схожих шаблонів (з найбільшими можливостями, отриманими при порівнянні). Потім, як і в попередньому випадку, з використанням будь-якого математичного критерію приймається рішення про ідентичність шаблонів. Така процедура називається **ідентифікацією** або **порівнянням "один до багатьох"**.

Всі біометричні системи працюють практично за однаковою схемою. По-перше, система запам'ятовує зразок біометричної характеристики (це і називається процесом запису). Під час запису деякі біометричні системи можуть попросити зробити декілька зразків для того, щоб скласти найбільш точне зображення біометричної характеристики. Потім отримана інформація обробляється і перетворюється в математичний код.

Крім того, система може попросити зробити ще деякі дії для того, щоб «приписати» біометричний зразок до певної людини. Наприклад, персональний ідентифікаційний номер (PIN) прикріплюється до певного зразка, або смарт-карта, яка містить зразок, вставляється в пристрій, що зчитує. У такому випадку знову робиться зразок біометричної характеристики і порівнюється з представленим зразком.

Ідентифікація за будь-якою біометричною системою проходить чотири стадії:

1. **Запис** – фізіологічний або поведінковий зразок запам'ятовується системою;
2. **Виділення** – унікальна інформація виноситься зі зразка і складається біометричний шаблон/еталон;
3. **Порівняння** – збережений зразок порівнюється з еталонним;
4. **Збіг / розбіжність** – система вирішує, чи збігаються біометричні зразки, і виносить рішення.

Варто також зазначити, що на відміну від аутентифікації суб'єктів за допомогою паролів або унікальних цифрових ключів, *біометричні системи завжди імовірнісні*, так як завжди зберігається малий, іноді вкрай малий шанс, що у двох людей можуть збігтися порівнювані біологічні характеристики. В силу цього біометрія визначає цілий ряд важливих термінів:

- **False Rejection Rate** (**FRR**, коефіцієнт помилкової відмови в доступі, також іменується як "помилка 1-го роду") – імовірність того, що суб'єкт може бути не розпізнаний системою, доступ заборонений користувачеві, зареєстрованому в системі [2].
- **False Acceptence Rate** (**FAR**, коефіцієнт помилкового допуску, також іменується як "помилка 2-го роду") – ймовірність того, що один суб'єкт може бути прийнятий за іншого, випадки надання системою доступу неавторизованому користувачеві [2].
- **Equal Error Rate** (**EER**, рівний рівень помилок) – це коефіцієнти, при яких обидві помилки ("помилка 1-го роду" та "помилка 2-го роду", **FRR = FAR**) еквівалентні. Зазвичай, пристрої з низьким EER найбільш точні. Чим менше EER, тим точнішою буде система [2].
- **Receiver Operating Characteristic** (**ROC curve**, крива ROC, крива помилок) – графік, що дозволяє оцінити компроміс між характеристиками FAR та FRR. У загальному випадку порівняльний алгоритм приймає рішення на підставі порога, який визначає, наскільки близько повинен бути вхідний зразок до шаблону, щоб вважати це збігом. Якщо поріг був зменшений, то буде менше помилок відмови в доступі, але більше помилкових допусків. Відповідно, високий поріг зменшить FAR, але збільшить FRR [2].

1.2 Класифікація біометричних методів аутентифікації

Нині широко використовується велика кількість методів біометричної аутентифікації. Розрізняють дві групи методів біометричної аутентифікації: статичні та динамічні.

Статичні методи засновані на фізіологічних характеристиках людини, присутніх від народження і до смерті, що знаходяться при ній протягом всього її життя, і які не можуть бути втрачені, вкрадені й скопійовані [3].

До них можна віднести:

- відбитки пальців
- форма/геометрія долоні
- розташування вен на тильній стороні долоні
- райдужна оболонка ока
- сітківка ока
- форма/геометрія обличчя (2D / 3D)
- термограма обличчя
- шкірне відображення/термограма тіла
- ДНК суб’єкта
- форма вух
- запах

Динамічні методи ґрунтуються на поведінкових характеристиках людини, тобто засновані на характерних підсвідомих рухах в процесі відтворення або повторення будь-якої звичайної дії [3].

До них можна віднести:

- голос
- рукописний почерк
- клавіатурний почерк
- хода
- рух губ


БІОМЕТРИЧНІ МЕТОДИ АУТЕНТИФІКАЦІЇ СУБ'ЄКТА
За принципом дії
Статичні методи
Динамічні методи
Відбитки пальців – 56 %
Форма/геометрія долоні – 7 %
Розташування вен на тильній стороні долоні – 3 %
Радужна оболонка ока – 7 %
Сітківка ока – 3%
Форма/геометрія обличчя (2D / 3D) – 18 %
Термограма обличчя - 2 %
Шкірне відображення – 1 %
ДНК суб'єкта – 1 %
Форма вух – 1 %
Запах – 1 %
Голос – 59 %
Рукописний почерк – 25 %
Клавіатурний почерк – 13 %
Хода – 2 %
Рух губ – 1 %

Рисунок 1.2 – Біометричні методи аутентифікації суб’єкта

1.3 Статичні методи

1.3.1 Відбитки пальців

Основна тема даної роботи пов’язана з дактилоскопією – розділ криміналістики, який займається дослідженням конфігурації папілярних ліній на пучках пальців рук із метою встановлення ідентичності. Метод ідентифікації людей за відбитками пальців (в т.ч. за слідами пальців рук), заснований на унікальності малюнка шкіри. Ідея методу заснована на гіпотезі про незмінність папілярного рисунку долонних поверхонь шкіри людини [3].

У кожному відбитку пальця можна визначити два типи ознак – глобальні та локальні.

Глобальні ознаки – це зовнішній вигляд відбитку, орієнтація зображення, кривизна і поле напрямків, яке описує загальне положення папілярних ліній відбитків пальців. Тобто це ті ознаки, які можна побачити неозброєним оком [4].

Об’єктом дослідження є папілярний візерунок – рельєфні лінії на долонях і підошовних поверхнях (включаючи пальці) у людей. Тобто:

- **Область візерунка** – виділений фрагмент відбитка, в якому локалізовані всі глобальні ознаки.
- **Ядро** або **центр** – точка, локалізована в середині відбитка або деякої виділеної області.
- **Пункт «дельта»** – початкова точка. Місце, в якому відбувається поділ або з'єднання борозенок папілярних ліній, або дуже коротка борозенка (може доходити до точки).
- **Тип лінії** – дві найбільші лінії, які починаються як паралельні, а потім розходяться і огинають всю область образу.
- **Лічильник ліній** – число ліній на області образу або між ядром і пунктом «дельта».

Одним із способів класифікації є розподіл відбитків пальців за типом папілярного візерунку. Відбитки бувають 3-х типів:

a) візерунок типу **«петля»** (ліва, права, центральна, подвійна)

b) візерунок типу **«дельта»** або **«дуга»** (проста і гостра)

c) візерунок типу **«спіраль»** (центральна і змішана)

а)

б)

в)

Рисунок 1.3.1 – Типи папілярних візерунків: а) петля, б) дельта, в) спіраль

Локальні ознаки або *мінуції* (*особливі точки* або *«точки Гальтона»*) – ділянки папілярного рисунку шкіри, в яких відбувається зміна структури папілярних ліній (закінчення, роздвоєння, розрив), за якими визначається приналежність відбитку пальця тій чи іншій людині. Іншими словами, це унікальні для кожного відбитку пальця точки, в яких змінюється структура папілярних ліній [4].

Кожен відбиток може містити до 70 і більше мінуцій, а загалом існує більше 150 видів мінуцій.

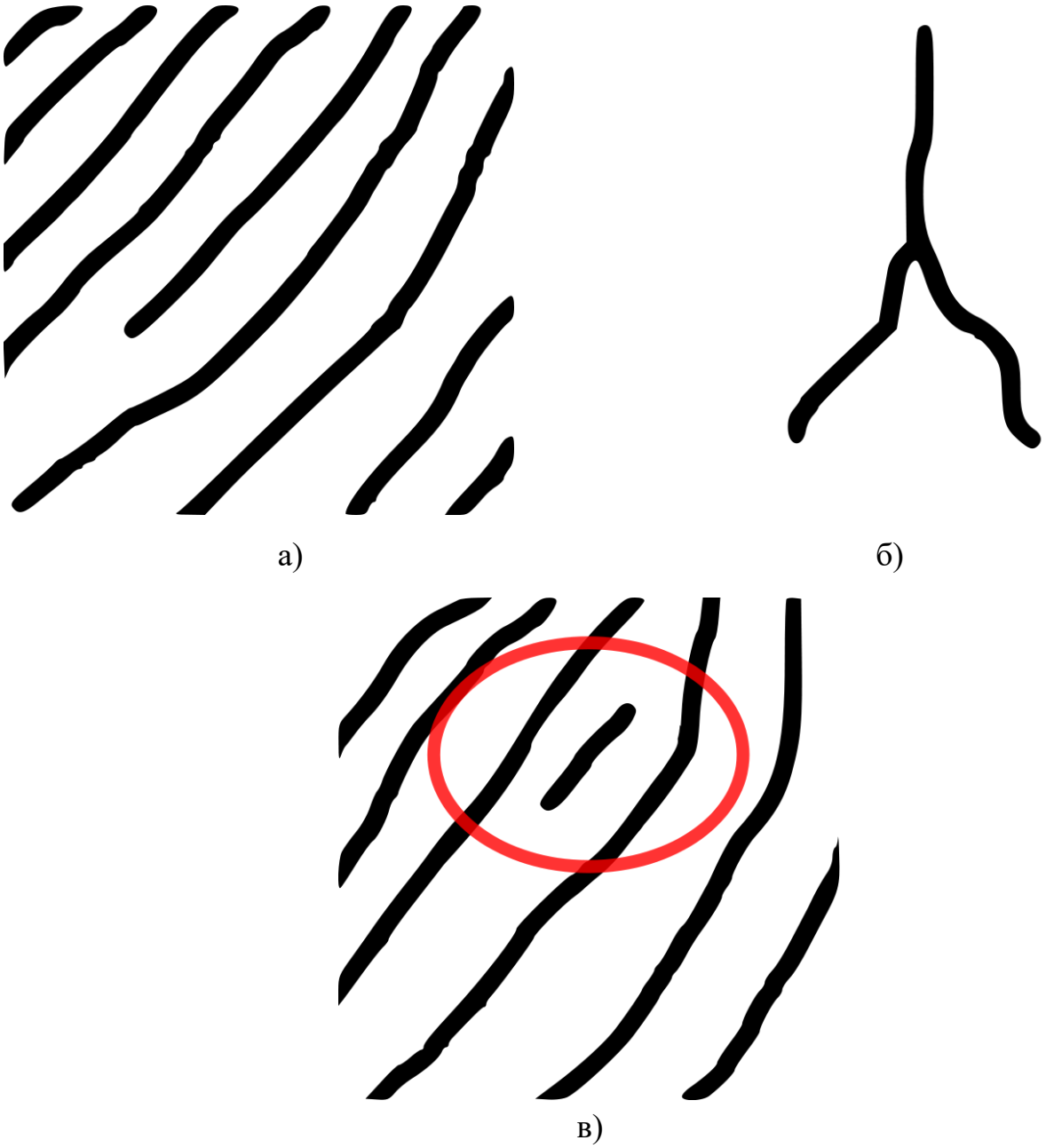

Рисунок 1.3.2 – Типи мінуцій: а) закінчення, б) роздвоєння, в) розрив

Практика показує, що відбитки пальців різних людей можуть мати однакові глобальні ознаки, але абсолютно неможливо наявність однакових мікровізерунків мінуцій. Тому глобальні ознаки використовують для поділу бази даних на класи і на етапи аутентифікації. На другому етапі розпізнавання використовують вже локальні ознаки.

Надалі в роботі буде розглядатися підхід на основі локальних ознак, так як він є найбільш поширеним в даний час та більш надійним, аніж підхід на основі глобальних ознак.

1.3.2 Форма/геометрія долоні

У даному методі біометричної аутентифікації суб’єкта використовується форма кисті руки. Через те, що окремі параметри форми руки не є чимось унікальним, доводиться використовувати кілька характеристик. Скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильної сторони долоні, відстань між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі (наприклад, зморшки на шкірі). Хоча структура суглобів і кісток є відносно сталими ознаками, але розпухання тканин або удари руки можуть спотворити вихідну структуру. Проблема технології: навіть без урахування можливості ампутації, захворювання під назвою «артрит» може сильно перешкодити застосуванню сканерів [3].

За допомогою сканера, який складається з камери і підсвічувальних діодів (при скануванні кисті руки діоди вмикаються по черзі, це дозволяє отримати різні проекції руки), потім будується тривимірний образ кисті руки. Надійність аутентифікації за геометрією руки порівняна з аутентифікацією за відбитком пальця.

Системи аутентифікації за геометрєю руки широко поширені, що є доказом їх зручності для користувачів. Використання цього методу є привабливим із ряду причин. Процедура отримання зразка досить проста й не пред'являє високих

вимог до зображення. Розмір отриманого шаблону дуже малий, кілька байт. На процес аутентифікації не впливають ні температура, ні вологість, ні забрудненість долоні. Підрахунки, зроблені при порівнянні з еталоном, дуже прості і можуть бути легко автоматизовані.

Системи аутентифікації, засновані на геометрії долоні, почали використовуватися в світі на початку 70-х років.

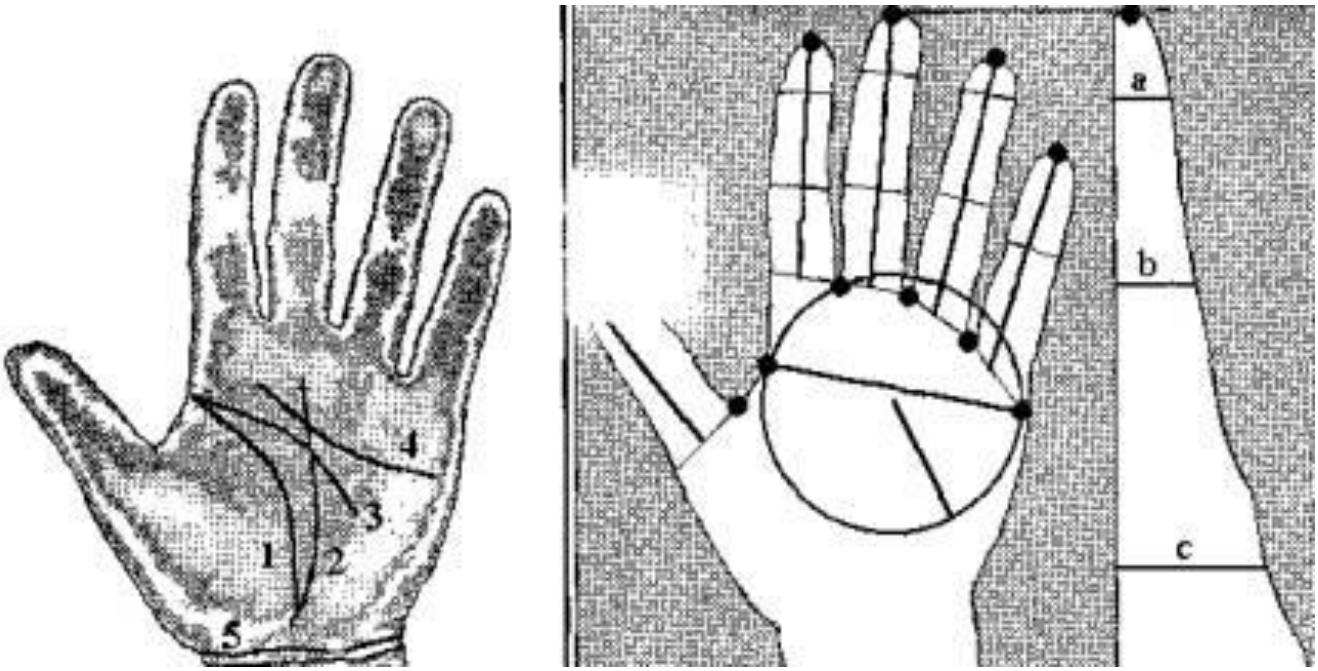

Рисунок 1.3.3 – Геометрія руки

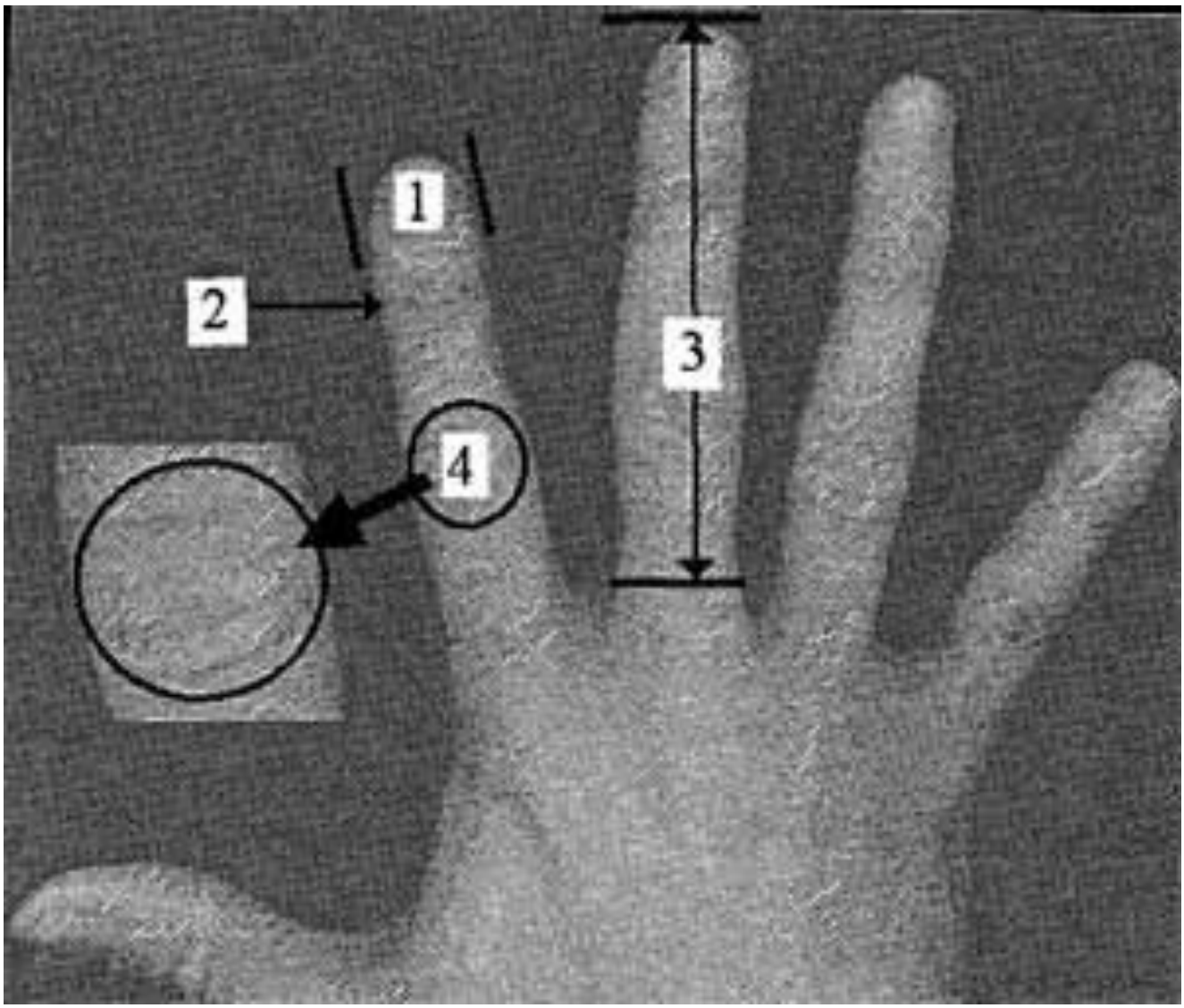

Рисунок 1.3.4 – Геометрія руки: 1) товщина пальця, 2) вигин пальця, 3) довжина пальця, 4) зморшки на шкірі

1.3.3 Розташування вен на тильній стороні долоні

Біометричні системи доступу засновані на людських параметрах, які завжди перебувати разом з ними, і проблема їх збереження не виникає. Втратити їх не можна. Також неможлива передача ідентифікатора третім особам. Втім, можна насильно вилучити параметри. У кінофільмах й анімації було неодноразово показано, що очі і руки можна ампутувати. Цього недоліку немає у *васкулярної аутентифікації*, яка дозволяє ідентифікувати тільки живу людину [3].

Васкулярний (медичний термін, від лат. Vascularis; від лат. Vasculum зменшувальне від vas –судина) – судинний; той, що відноситься до судин.

Васкулярна аутентифікація, яка використовує розпізнавання зображень і оптичну технологію для сканування зазвичай невидимих структур вен долоні (рис. 1), тильної сторони долоні, пальців і т.д., має властивості високого ступеня точності і високу стійкісь до підробки, підміни та інших зловмисних дій.

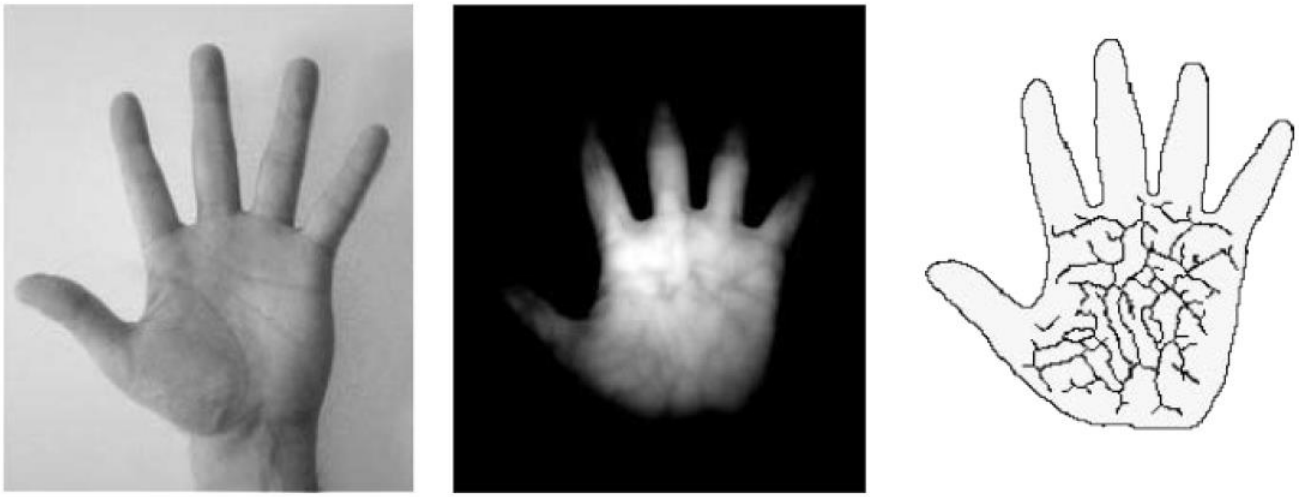

Рисунок 1.3.5 – Генерування зображення долоні людини в інфрачервоному діапазоні й перетворення даних для зберігання в зашифрованому вигляді

З доступних актуальних біометричних рішень аутентифікація за венами долоні передбачає кращу точність і безпеку. Візерунки кровоносних судин є унікальними для кожної людини. Це досить нова технологія у сфері біометрії, широке застосування її почалося всього років 5-10 тому.

Найголовніше те, що ці судинні візерунки існують всередині тіла, а не зовні. Вони не можуть бути вкрадені за допомогою фотографії, підробки або інших подібних методів, що робить цей метод біометричний аутентифікації набагато безпечнішим, ніж інші.

Коли долоня освітлюється світлом, близьким до інфрачервоного, знекиснений гемоглобін всередині вен поглинає це світло, проявляючи вени як темний малюнок поверх іншого зображення. Таким чином, область долоні, яка

використовується для аутентифікації, фотографується в близькому до інфрачервоного світлі, й зразок візерунка вен витягується шляхом обробки зображення і розпізнавання. Щоб авторизувати користувача, його унікальні зразки візерунків вен звіряються з раніше зареєстрованими зразками, що зберігаються в базі даних, на смарт-карті або в зашифрованому вигляді на інших носіях інформації.

Рисунок 1.3.6 – Зображення вен долоні людини в інфрачервоному діапазоні

Існує два методи отримання зображення малюнка вен долоні. *Метод відображення (Reflection)* дозволяє розмістити всі компоненти пристрою в одному корпусі, за рахунок чого зменшується розмір. Також знижується психологічний бар'єр (не потрібно нікуди засовувати руку). *Метод пропускання*

інфрачервоного світла (Transmission) полягає в установці інфрачервоного підсвічування з тильного боку долоні, а сама камера з фільтром встановлюється з боку долоні і приймає інфрачервоне випромінювання, що проходить через всю долоню. За допомогою методу пропускання одержувані зображення більш деталізовані.

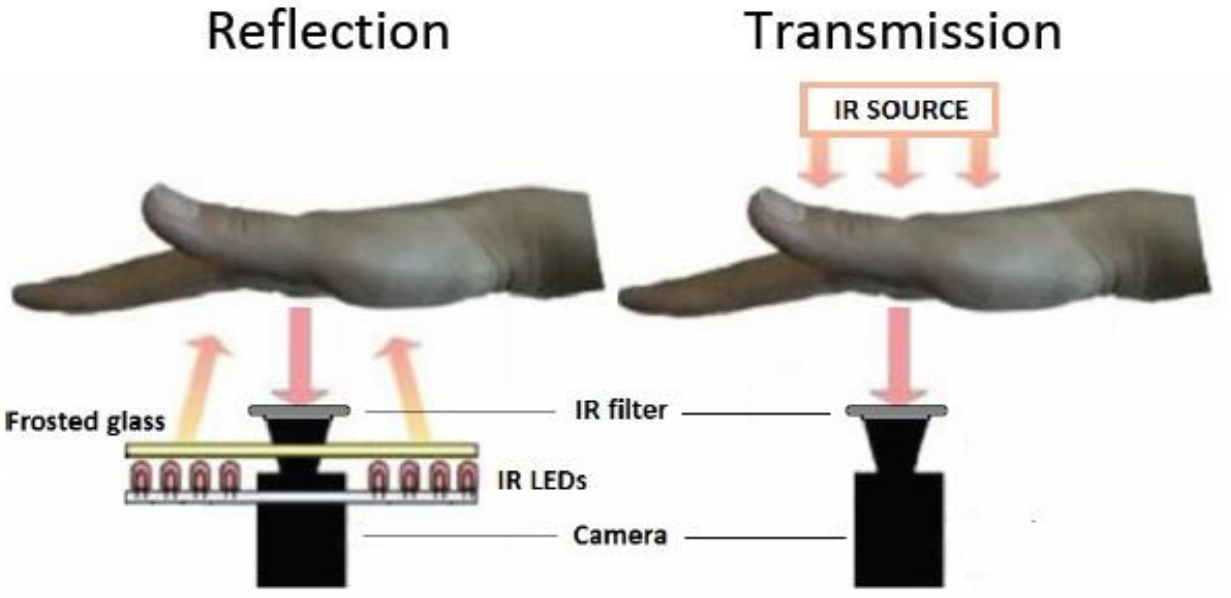

Рисунок 1.3.7 – Методи отримання зображення вен долоні: *відображення* (зліва), *пропускання* (справа)

В результаті, ступінь відображення зменшується, і вени видно на камері у вигляді чорних ліній. Спеціальна програма на основі отриманих даних створює цифрову згортку. Не потрібно контакту людини з скануючим пристроєм.

Технологія порівнянна за ефективністю з розпізнаванням за райдужною оболонкою ока, в чомусь перевершуючи її, а в чомусь поступаючись.

Значення FRR і FAR наведено для сканера Palm Vein. Згідно з даними розробника при FAR 0,0008% FRR становить 0.01%. Більш точний графік для кількох значень не видає жодна фірма.

1.3.4 Радуйжна оболонка ока

Дана технологія біометричної аутентифікації особистості використовує унікальність ознак і особливостей райдужної оболонки ока. Райдужна оболонка – це тонка рухома діафрагма ока, з отвором (зіницею) в центрі; розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Райдужна оболонка утворюється ще до народження людини і не змінюється протягом усього життя. Райдужна оболонка за текстурою нагадує мережу з великою кількістю оточуючих кіл і рисунків, які можуть бути виміряні комп'ютером, рисунок райдужної оболонки дуже складний, це дозволяє відібрати близько 200 точок, за допомогою яких забезпечується високий ступінь ефективності аутентифікації. Для порівняння, кращі системи ідентифікації за відбитками пальців використовують 60-70 точок [3].

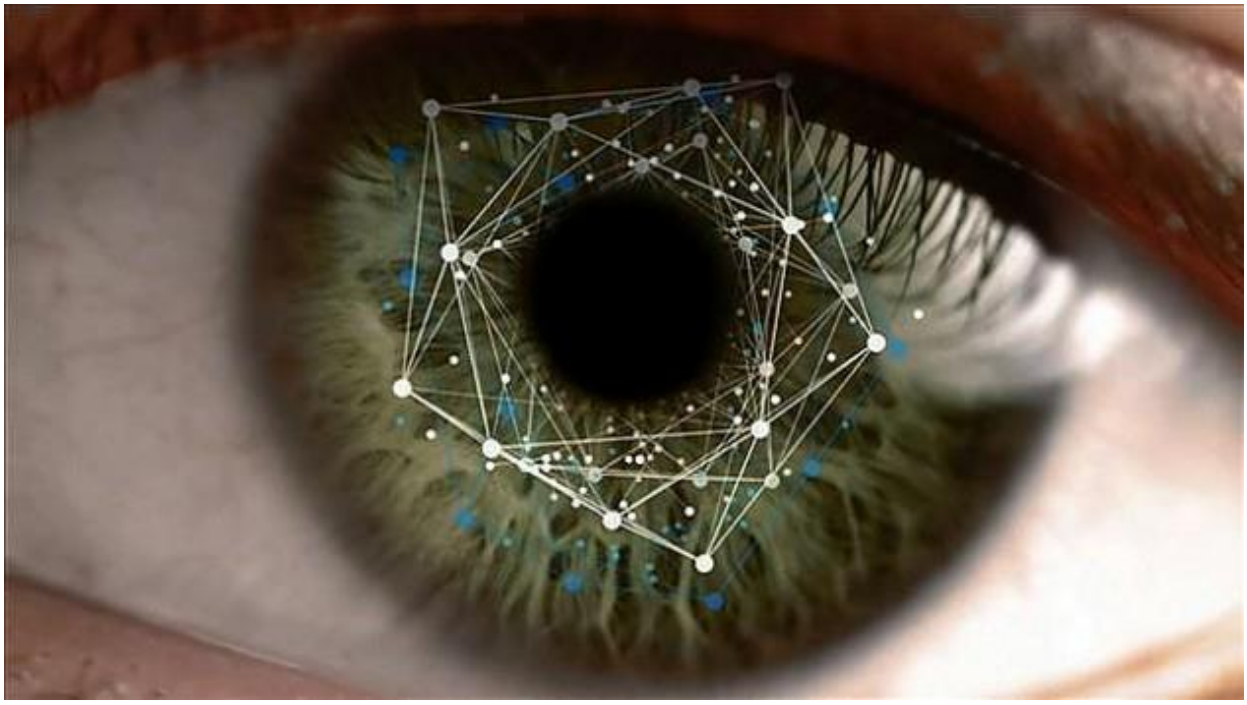

Рисунок 1.3.8 – Унікальні точки райдужної оболонки ока

Технологія розпізнавання райдужної оболонки ока була розроблена для того, щоб звести нанівець нав'язливість сканування сітківки ока, при якому використовуються інфрачервоні промені або яскраве світло. Вчені також провели

ряд досліджень, які показали, що сітківка ока людини може змінюватися з часом, в той час як райдужна оболонка ока залишається незмінною. І найголовніше, що неможливо знайти два абсолютно ідентичних рисунки райдужної оболонки ока, навіть у близнюків. Для отримання індивідуального запису про райдужну оболонку ока чорно-біла камера робить 30 записів на секунду. Ледве помітне світло висвітлює райдужну оболонку, і це дозволяє відеокамері сфокусуватися на райдужці. Один із записів потім оцифровується і зберігається в базі даних зареєстрованих користувачів. Вся процедура займає кілька секунд, і вона може бути повністю комп'ютеризована за допомогою голосових вказівок і автофокусування. Камера може бути встановлена на відстані від 10 см до 1 метра, в залежності від скануючого обладнання. Термін «сканування» може бути оманливим, оскільки в процесі отримання зображення проходить не сканування, а просте фотографування. Потім отримане зображення райдужної оболонки перетворюється в спрощену форму, записується і зберігається для подальшого порівняння. Окуляри та контактні лінзи, навіть кольорові, не впливають на якість аутентифікації.

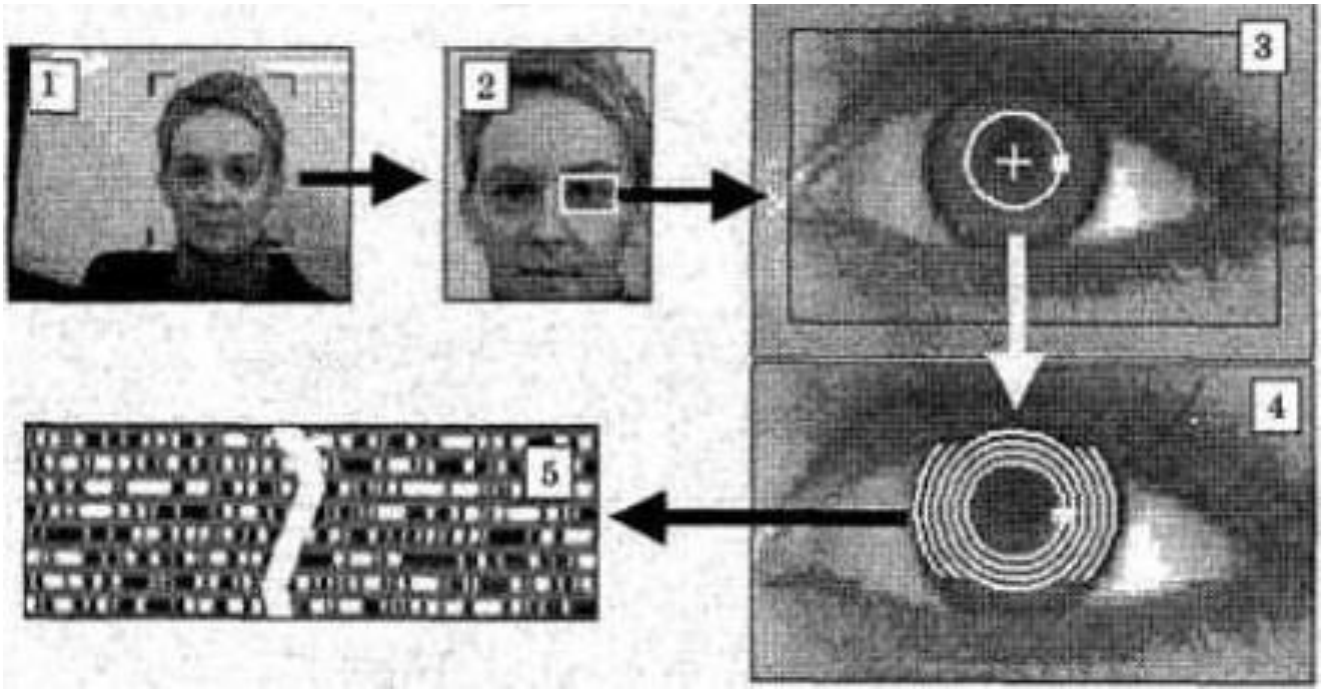

Рисунок 1.3.9 – Етапи процесу розпізнавання особи за райдужною оболонкою ока

1.3.5 Сітківка ока

Метод аутентифікації за сітківкою ока отримав практичне застосування приблизно в середині 50-х років минулого століття. Саме тоді була встановлена унікальність рисунка кровоносних судин очного дна (навіть у близнюків дані малюнки не збігаються). Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, спрямоване через зіницю до кровоносних судин на задній стінці ока. З отриманого сигналу виділяється кілька сотень особливих точок, інформація про які зберігається в шаблоні [3].

До недоліків таких систем слід в першу чергу віднести психологічний фактор: не кожній людині приємно дивитися в незрозумілий темний отвір, де щось світить в око. До того ж, подібні системи вимагають чіткого зображення і, як правило, чутливі до неправильної орієнтації сітківки. Тому потрібно дивитися дуже акуратно, а наявність деяких захворювань (наприклад, катаракти) може перешкоджати використанню даного методу. Сканери для сітківки ока набули великого поширення для доступу до надсекретних об'єктів, оскільки забезпечують одну з найнижчих ймовірностей помилки першого роду (відмова в доступі для зареєстрованого користувача) і майже нульовий відсоток помилок другого роду.

1.3.6 Форма/геометрія обличчя (2D / 3D)

Біометрична аутентифікація людини за геометрією особи – досить поширений спосіб ідентифікації і аутентифікації. Технічна реалізація представляє собою складну задачку. Широке застосування мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя, виділяють контури очей, брів, губ, носа та інших різних

елементів особи, потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель. Щоб знайти цей унікальний шаблон, що відповідає певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу. Діапазон таких варіантів варіюється в залежності від цілей застосування даного способу (для ідентифікації, аутентифікації, віддаленого пошуку на великих територіях і т. д.). Деякі алгоритми дозволяють компенсувати наявність у людини окулярів, капелюху, вусів і бороди [3].

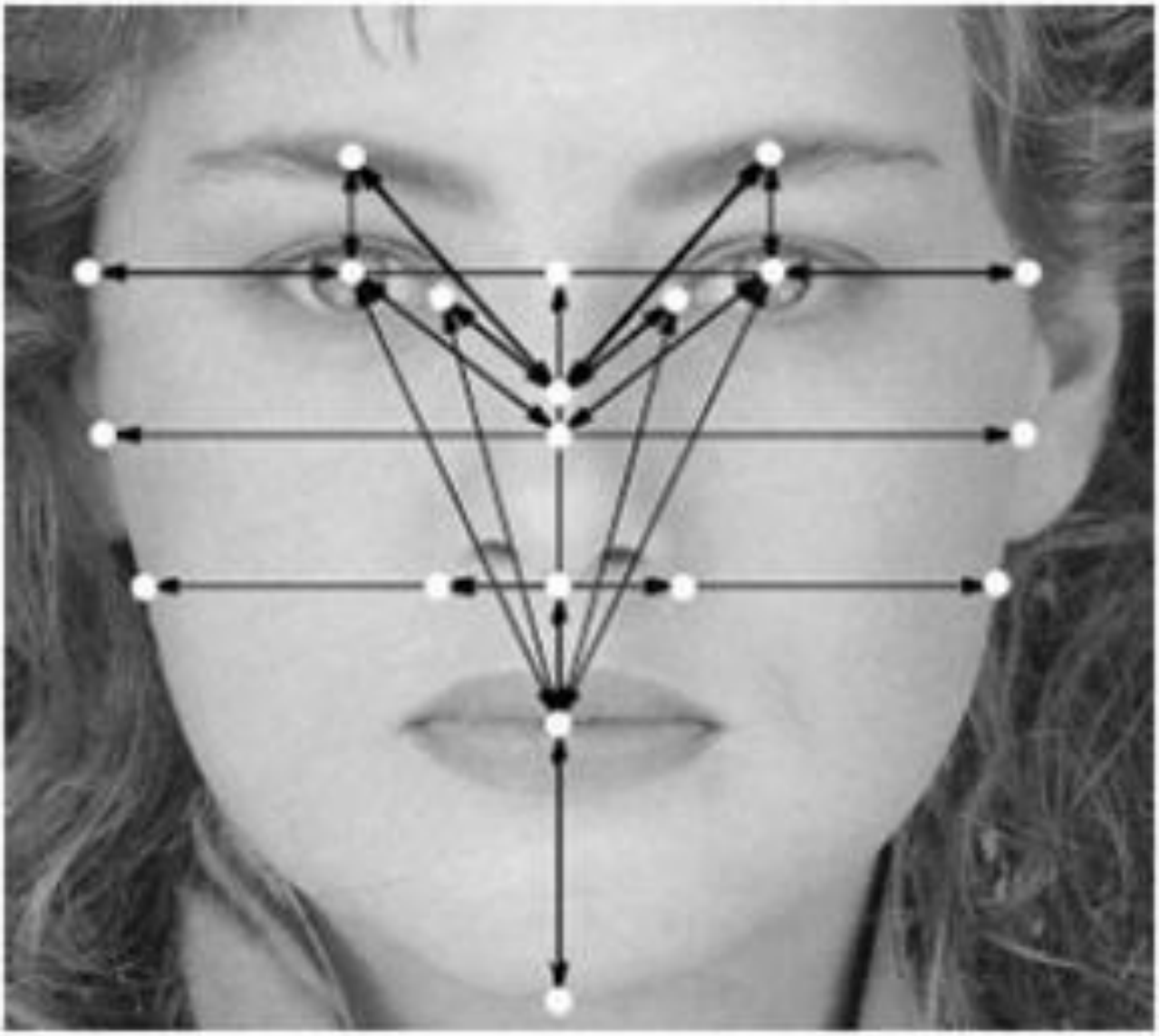

Рисунок 1.3.10 – 2-D розпізнавання обличчя

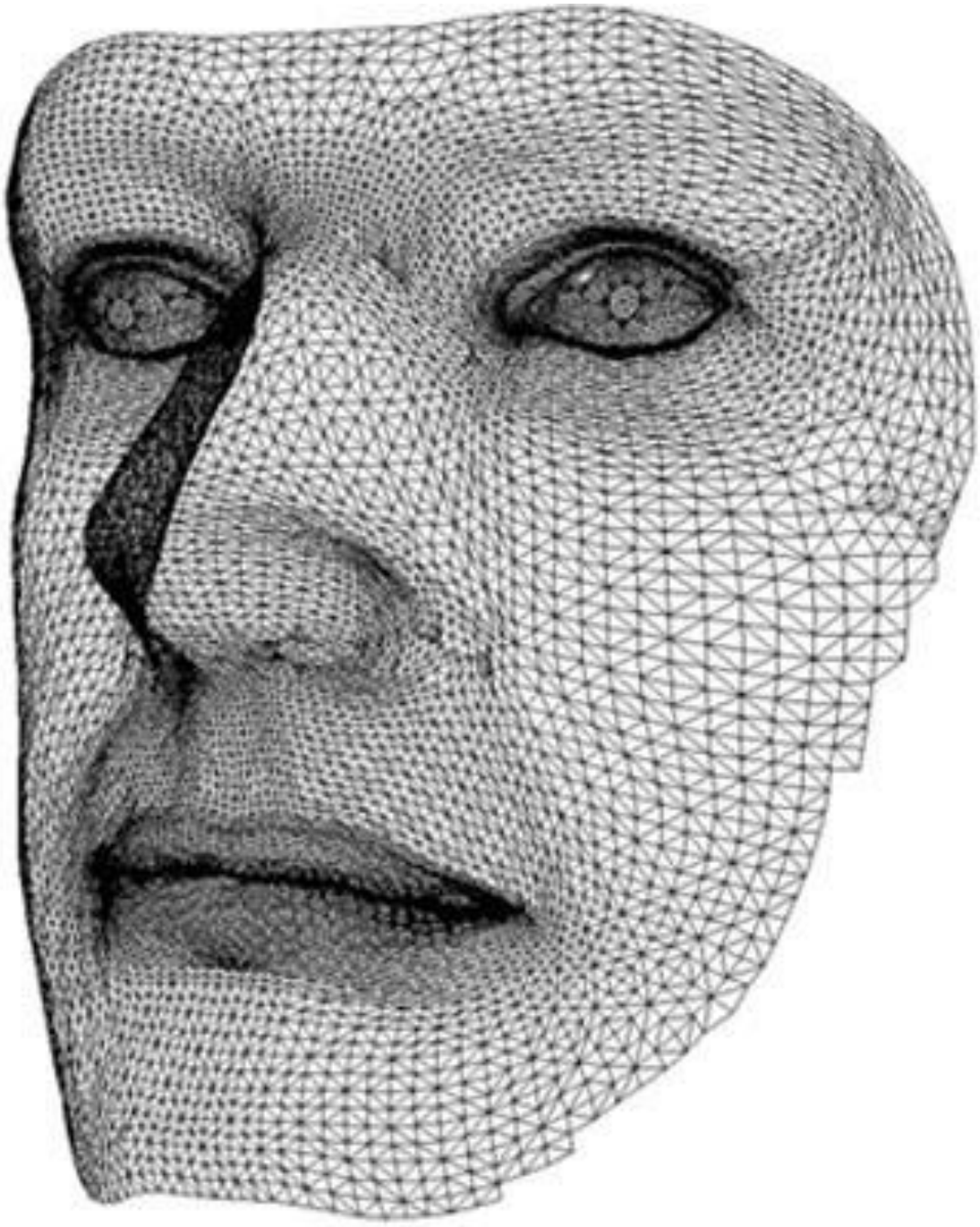

Рисунок 1.3.11 – 3-D розпізнавання обличчя

1.3.7 Термограма обличчя

Спосіб заснований на дослідженнях, які показали, що термограма особи унікальна для кожної людини. Термограма виходить за допомогою камер інфрачервоного діапазону. На відміну від аутентифікації за геометрією особи,

даний метод розрізняє близнюків. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Через невисоку якість аутентифікації, метод на даний момент не має широкого поширення [3].

Системи дозволяють ідентифікувати людину на відстані до десятків метрів. У комбінації з пошуком даних по базі даних такі системи використовуються для впізнання авторизованих співробітників і відсіювання сторонніх. Однак при зміні освітленості сканери особи мають відносно високий відсоток помилок.

1.3.8 Додаткові біометричні параметри

Шкірне відображення

Один з нових біометричних параметрів, що з'явився завдяки розробці нових сенсорів, – відображення шкіри. У цій методиці використовується маленький чіп, розроблений корпорацією «Люмідінм» (Lumidinm), за допомогою якого вимірюється відображення від шкіри ближнього інфрачервоного світла в діапазоні з довжиною хвилі більше 6 мм. Досі дана технологія аутентифікації застосовується окремо, але в комбінації з розпізнаванням за відбитками пальців вона могла б забезпечити захист від підробок. Перевагою даної технології є те, що для зразка маленького розміру потрібно і маленький чіп – за розміром і об’ємом пам'яті і продуктивності. Також потрібно відзначити відсутність проблем з реєстрацією, які характерні для методу аутентитифікації за відбитками пальців [3].

ДНК суб’єкта

ДНК часто називають майже ідеальним біометричних параметром, так як код ДНК є ідентифікаційною інформацією в цифровій формі, яка є в будь-якій клітині людини. Недолік цього параметра в тому, що однояйцеві близнюки будуть мати одну і ту ж ДНК. Крім того, з практичної точки зору порівняння людей на

основі двох зразків ДНК – повільний (займає години або дні), дорогий і складний процес. Досі використання ДНК як біометричного параметра обмежена в основному сферою судової експертизи, для якої поява методу ідентифікації за ДНК стало справжньою революцією. Аналіз ДНК також використовується для встановлення споріднення (для ідентифікації, встановлення батьківства або генетичних досліджень). Існує і багато інших можливостей для застосування цього методу [3].

Основою ідентифікації за ДНК слугує порівняння альтернативних форм (алелей) ланцюжка ДНК на ідентифікованих точках (локусах) ядерного генетичного матеріалу. Хоча близько 99,5 % людського генетичного матеріалу є однаковим для всіх людей, існує множина локусів, які можна використовувати для ідентифікації суб'єкта. У процесі ідентифікації досліджується набір локусів з метою визначення представлених у кожному з них аллелей (зазвичай, в одному локусі є дві різні аллелі – по одній в кожній хромосомі).

Будь-яке розходження між зареєстрованим і тестовим зразками говорить про те, що вони належать різним людям, ймовірність їх збігу можна розрахувати. Звичайні тести оцінюють ймовірність повного збігу як один до трильйона з умовою, що близькі родичі (особливо близнюки) можуть бути виключені з інших підстав.

Якщо в локусі розташовано 50 різних аллелей, то людина може мати 1275 можливих пар цих аллелей. Якщо розглянути 4 незалежних локуси, вийде 2,6 трильйона комбінацій. Звичайно, ідентифікація за ДНК потребує гарантії чистоти зразків і того, що зразки не переплутаються в процесі проходження процедур.

Конфіденційність – одна з головних проблем при ідентифікації по ДНК, так як в ДНК закодована інформація, яка може бути використана для інших цілей – незаконного отримання інформації про медичні показання і схильності людини до хвороб, а також про расову приналежність і батьківство. Інформація про те, яка аллель знаходиться в кожному локусі, не має великої цінності, на відміну від повного ланцюжка ДНК, представленого в оригінальному зразку.

Форма вух

Вимірювання вух було частиною системи Бертильона, в якій вчені спостерігачі визначали тип форми вух, щоб використовувати його як один з індексів у великій біометричній системі. Існують навіть випадки застосування латентних відбитків вух для ідентифікації злочинців. Останнім часом більше уваги приділяється формі вух в якості біометричного параметра для автоматичної ідентифікації. Одна група дослідників використовувала техніку знаходження країв для отримання основної структури вуха, необхідної для проведення порівняння. Ці автори також застосовували термограми для виключення залежності зображення від освітлення і волосся [3].

Додатковий інтерес до розпізнавання за формою вух виник у зв'язку з проектом «Ідентифікація людини на відстані».

Аналіз основних елементів вух схожий на систему аналізу за допомогою «особистих осіб». Використання тільки методики розпізнавання за формою вух не так ефективно, як розпізнавання за обличчям; комбінація зображень «обличчя плюс вухо» підвищує точність ідентифікації.

Запах

Уже давно відомо, що людину можна ідентифікувати за його особистим запахом. Прогрес в області хімічного аналізу з застосуванням напівпровідників призвів до винаходу «електронних носів», які можуть вимірювати концентрацію різних хімічних елементів (всього 32). Такі сенсори, звичайно, не володіють ні розпізнавальною здатністю, ні чуттєвістю людського носа й мають свої недоліки – потребують калібровки, погано працюють в умовах перевантаження (при наявності безлічі різних запахів може статися навіть «отруєння»). Також відомо, що запах людини залежить від його способу життя – починаючи від харчування й стану здоров'я, закінчуючи використанням мила, парфумерії та дезодорантів. Поки що невідомо, чи можна нормалізувати ці фактори настільки, щоб надійна ідентифікація людини за запахом стала можливою [3].

1.4 Динамічні методи

1.4.1 Голос

Голос – це поведінковий біометричний параметр, що залежить від фізичних характеристик. Властивості голосу, такі, як частота, носовий звук, модуляція, інтонація і т.д., є унікальними особливостями людини [3].

Ідентифікація людини за голосом – один з традиційних способів розпізнавання, який застосовується повсюди. Можна легко дізнатися про співрозмовника по телефону, не бачачи його. Також можна визначити психологічний стан за емоційним забарвленням голосу.

Біометричний метод аутентифікації за голосом характеризується простотою в застосуванні. Даному методу не потрібно дорога апаратура, досить мікрофона і звукової плати. В даний час дана технологія швидко розвивається, так як цей метод аутентифікації широко використовується в сучасних бізнес-центрах. Існує досить багато способів побудови шаблону за голосом. Зазвичай, це різні комбінації частотних і статистичних характеристик голосу. Можуть розглядатися такі параметри, як модуляція, інтонація, висота тону тощо.

Основний і визначальний недолік методу аутентифікації за голосом – низька точність методу.

Голос схильний до суттєвих змін під впливом емоційних чинників (настрій людини) і стану здоров'я (ангіна, нежить, бронхіт і т.д.). На якості ідентифікації можуть позначатися зовнішні умови (наприклад, сторонні шуми від дорожнього руху, розмов інших людей). Якщо для передачі голосової інформації використовуються лінії зв'язку, перешкоди в них також здатні ускладнити розпізнавання суб’єкта.

Це різноманіття представляє серйозні труднощі при виділенні характерних властивостей голосу людини. Крім того, врахування шумових компонентів є ще

однією важливою і невирішеною проблемою в практичному використанні аутентифікації по голосу.

Існуючі системи розпізнавання людини за голосом мають такі характеристики: помилки першого роду (недопуск свого) складають від 1 до 5% (хоча, залежно від реалізації програмного забезпечення, можуть доходити й до 40%). Кількість помилок другого роду (пропуск чужого) залежить від того, чи знає зловмисник ключову фразу (до 1%, якщо голоси близькі) чи ні (0,00000001%). Зараз можна використовувати голосову аутентифікацію спільно з іншими видами захисту. Наприклад, за геометрією обличчя. Тоді можна відстежувати рух губ і синхронізацію їх зі звуком.

Аутентифікація за голосом застосовується для управління доступом в приміщеннях середнього рівня безпеки, такі як комп'ютерні класи, лабораторії виробничих компаній і т. д.

1.4.2 Рукописний почерк

Метод біометричної аутентифікації за рукописним почерком ґрунтується на специфічному русі людської руки під час підписання документів. Для збереження підпису використовують спеціальні ручки або сприйнятливі до тиску поверхні. Цей вид аутентифікації людини використовує його підпис. Шаблон створюється в залежності від необхідного рівня захисту. Зазвичай, виділяють два способи обробки даних про підписи:

1. **статичний** – аналіз самого підпису, тобто використовується просто ступінь збігу двох картинок;
2. **динамічний** – аналіз динамічних характеристик написання, тобто для аутентифікації будується згортка, в яку входить інформація щодо підпису, тимчасових і статистичних характеристик його написання.

Перший спосіб досить ненадійний, тому що заснований на звичайному порівнянні введеного підпису з графічним зразком, який зберігається в базі даних.

Через те, що підпис не може бути завжди однаковим, цей метод дає великий відсоток помилок. Спосіб динамічної верифікації вимагає набагато складніших обчислень і дозволяє в реальному часі фіксувати параметри процесу підпису, такі як швидкість руху руки на різних ділянках, сила тиску і тривалість різних етапів підпису. Це дає гарантії того, що підпис не зможе підробити навіть досвідчений графолог, оскільки ніхто не в змозі в точності скопіювати поведінку руки власника підпису. Тільки справжній користувач зможе повторити всі ці характеристики за той же час. Копіювальна машина або спеціаліст можуть з легкістю зробити дублікат вашого підпису і відтворити його, але дублювати час і всі характеристики підпису практично неможливо [3].

Відпрацьована згодом манера особистого підпису людини є необхідною характеристикою для відтворення всіх необхідних параметрів, які потім і розглядає система. Кожен раз, підписуючи документи, в підписі можуть бути якісь невеликі варіації, але характеристики, які визначаються природними рухами і особливостями, виробленими протягом довгого часу, створюють впізнавані характеристики, які і роблять підпис об'єктом для біометричної ідентифікації.

Користувач, використовуючи стандартний дігітайзер і ручку, імітує свій звичайний підпис, а система зчитує параметри руху і звіряє їх з тими, що були заздалегідь введені в базу даних.

Деякі методи враховують дані про коливання пера при відтворенні підпису в тривимірному просторі (X, Y – координати й Z – тиск на планшет). Системи, що використовують одну з функцій часу $X(t)$, $Y(t)$ або $Z(t)$, забезпечують вірогідність помилок 0,1. Якщо використовувати дві функції, то 0,01. Для трьох функцій – 0,003.

Інші системи використовують не самі функції, а їх першу або другу похідну. Що, втім, має незначний вплив на якість розпізнавання.

Іноді використовуються і більш складні сенсори. Ці пристрої записують напрямок п’яти вимірних векторів (x, y, p, θ_X, θ_Y), взятих в еквідистантних точках часу. Тут p – це осьовий тиск ручки, а θ_X та θ_Y – це кут ручки в площині X-Y. Ця додаткова інформація дуже важлива для запобігання фальсифікаціям.

Динамічна верифікація підпису включає в себе вимір евклідової відстані між траєкторією ручки, параметрами просторових взаємозв'язків і т.д. При збігу образу підпису з еталоном система прикріплює до підписуючого документа параметри підпису, що містять декілька десятків характеристик динаміки руху (напрямок, швидкість, прискорення) та інші. Ці дані шифруються, потім для них обчислюється контрольна сума, і далі все це шифрується ще раз, утворюючи так звану біометричну мітку. Для налаштування системи знову зареєстрований користувач від п'яти до десяти разів виконує процедуру підпису документа, що дозволяє отримати усереднені показники й довірчий інтервал.

1.4.3 Клавіатурний почерк

Ідентифікація за клавіатурним почерком – це ідентифікація людини за його власним стилем друку. Кожна людина має характерні особливості друку: час між натисканням клавіш і час утримання клавіші є більш-менш постійним для кожної людини і відрізняє її від інших людей [3].

Існує система на базі штучних нейронних мереж для розрізнення 15 людей за клавіатурним почерком. Дослідники помітили, що різниця між людьми більш помітна, якщо використовувати для розпізнавання тимчасові інтервали між натисканням клавіш і час утримання однієї клавіші.

Системи ідентифікації за клавіатурним почерком засновані на введенні фіксованого слова, але, ймовірно, можуть бути і незалежними від тексту, що набирається, як системи розпізнавання голосу.

В одній з дослідницьких робіт пропонується метод ідентифікації за клавіатурним почерком на основі змінних віртуальних клавіатур. Суть методу полягає в наступному.

При колективній роботі в автоматизованих інформаційно-керуючих системах кожному оператору надається своя персональна віртуальна клавіатура, яка відображається на екрані його комп'ютера. Вид і склад цієї клавіатури може

бути довільним, наприклад, таким же, як і стандартна, але розташування клавіш на клавіатурі відрізняється для кожного оператора. Вид клавіатури генерується системою або через заздалегідь підготовлений список, або на основі реалізації деякого алгоритму, або випадково. Кожен оператор повинен протягом досить тривалого часу працювати на «своїй» віртуальній клавіатурі, наданій йому системою. Набір символів на віртуальній клавіатурі може виконуватися шляхом переміщення курсору на екрані одним з двох способів:

1 мишею – натисканням відповідних віртуальних клавіш кнопкою миші;
2 п'ятьма клавішами на реальній клавіатурі комп'ютера (стрілки вгору, вниз, вправо, вліво, введення).

Оператор, який досить тривалий час працює на «своїй» віртуальній клавіатурі, набуває індивідуальних навичок, які виражаються в певній картині швидкостей введення окремих символів і тексту в цілому. У такій ситуації спроби підміни оператора добре ідентифікуються системою аналізу клавіатурного почерку.

1.4.4 Хода

Хода відноситься до поведінкових біометричних параметрів, вона вивчена ще мало. Переваги цього методу – можливість розпізнавання людей на відстані, використовуючи відеозаписи. У перших дослідженнях ідентифікація проводилася за допомогою обладнання, що зчитує рухи суб’єкта. Пізніші дослідження також засновані на спостереженні за людьми на спонтанно знятому відео [3].

Завдяки новим дослідженням, механізми розпізнавання за ходою стали більш досконалими. Дослідження проводилися на маленьких групах; виявилося, що результати розпізнавання залежать від багатьох факторів: поверхні, по якій іде людина, точки спостереження, взуття, швидкості переміщення людини і, звичайно, її фізичного здоров'я. Деякий одяг (особливо спідниці) може ускладнювати розпізнавання.

Всебічне дослідження методу розпізнавання людини за ходою проведено на основі великої бази даних (452 відеозаписів 74 об'єктів). Основний алгоритм розпізнавання:

1. спочатку напівавтоматично визначаються обмежуючі прямокутники, по яким йде об'єкт;
2. потім з них витягуються силуети;
3. третій крок – це зведення обмежуючих прямокутників до розміру 128×88 пікселів, для того, щоб виконати зіставлення шляхом «кореляції» силуетів.

Розроблено так званий "гайд-код" – код ходи, який вираховується після поділу за спеціальними фільтрами характерних і випадкових рухів, зафіксованих вбудованими сенсорами. В ході випробувань точність такого способу ідентифікації перевищувала 90%.

Процедура розпізнавання дуже сильно залежить від умов, в яких знаходиться об'єкт, наприклад: буде складно розпізнати людину, що йде по будь-якій поверхні (наприклад, по бетону), якщо система була навчена на основі відеозапису тієї ж людини, що йде по іншій поверхні (скажімо, по траві). Ця область біометрії вимагає подальшого вивчення.

1.4.5 Рух губ

Рух губ під час розмови відноситься до поведінкових біометричних параметрів. Він може використовуватися як візуальне доповнення до системи розпізнавання розмовника; технологія аутентифікації за рухом губ має такі ж різновиди, що і методика розпізнавання розмовника: з фіксованим текстом, залежно від тексту й незалежно від тексту. Останнім часом стало проводитися більше досліджень в даній області завдяки поширенню доступних баз даних [3].

На ринку представлена біометрична система компанії *“BioId”*, що використовує рух губ. Одна з найбільших переваг цього методу – можливість

легко поєднати його з ідентифікацією розмовника і розпізнанням за геометрією обличчя. Таким чином, можна створити дуже точну систему, яку буде складно обдурити. Подібна потрійна біометрична система призначена для контролю фізичного доступу, вона зчитує параметри людини, що говорить в мікрофон перед камерою. Відеозображення використовується для аналізу геометрії обличчя і руху губ, результати якого інтегруються з результатами розпізнавання за голосом.

При певному освітленні і високій якості зображення можна отримати дуже хороший відеозапис руху губ. Проте, коли умови зйомки погані, визначити положення губ у відеозображенні, отриманому в діапазоні видимого світла, буває досить складно.

Для отримання відеозображення рухів губ може використовуватися світло невидимого діапазону:

1. інфрачервоне світло: якщо потрібен високий рівень безпеки, то можна додати теплові зображення. Це ж стосується розпізнавання ходи і форми вух;
2. довгохвильове інфрачервоне світло: коли потрібне недороге рішення, можна використовувати контрольоване довгохвильове інфрачервоне освітлення.

Цей особливий тип активного зчитування, як і будь-яка спроба контролю зображення, робить процес отримання біометричного зразка помітним і менш придатним для типу прихованого сортування.

1.5 Аналіз

Одна з найважливіших характеристик систем захисту інформації, заснованих на біометричних технологіях, є їх висока надійність, тобто здатність системи достовірно розрізняти біометричні характеристики, що належать різним людям, і надійно знаходити збіги. У біометрії ці параметри називаються

помилкою першого роду (False Reject Rate, FRR) і помилкою другого роду (False Accept Rate, FAR).

Підробити папілярний візерунок пальця людини або райдужну оболонку ока дуже складно. Так що виникнення "помилок другого роду" (тобто надання доступу людині, яка не мала на це право) практично виключено. Однак, під впливом деяких факторів біологічні особливості, за якими проводиться ідентифікація суб'єкта, можуть змінюватися. Наприклад, людина може застудитися, в результаті чого її голос зміниться до невпізнання. Тому частота поява "помилок першого роду" (відмова в доступі людині, яка має на це право) в біометричних системах досить велика. **Система тим краща, чим менше значення FRR при однакових значеннях FAR.**

Іноді використовується і порівняльна характеристика EER (Equal Error Rate), яка визначає точку, в якій графіки FRR і FAR перетинаються. Але вона далеко не завжди є репрезентативною. При використанні біометричних систем, особливо системи розпізнавання за формою обличчя, навіть при введенні коректних біометричних характеристик не завжди рішення про аутентифікацію вірно. Це пов'язано з рядом особливостей і, в першу чергу, з тим, що багато біометричних характеристик можуть змінюватися. Існує певний ступінь ймовірності помилки системи. Причому при використанні різних технологій помилка може мати відчутні відмінності. Для систем контролю доступу при використанні біометричних технологій необхідно визначити, що важливіше – не пропустити "чужого" чи пропустити всіх "своїх".

Ідеальна біометрична характеристика повинна мати наступні властивості:

- *універсальність* – можливість представлення суб'єкта однією єдиною характеристикою;
- *унікальність* – виключення можливості існування двох суб'єктів з ідентичними характеристиками;
- *незмінність* – незалежність характеристики від часу і (відносно) від зовнішніх умов;

- *вимірність* – можливість швидкого і легкого отримання біометричної характеристики;
- *надійність* – рівень помилок біометричної системи;
- *ціна* – вартіть біометричної системи.

У таблиці 1.1 показані експертні оцінки властивостей характеристик людини.

Таблиця 1.1 – Експертні оцінки властивостей біометричних характеристик людини: 3 – висока оцінка, 2 – середня, 1 – низька.

Таблиця 1.1 – Експертні оцінки властивостей біометричних характеристик людини

Властивість / **Біометрична характеристика**	***Універсальність***	***Унікальність***	***Незмінність***	***Вимірність***	***Надійність***		***Ціна***
					FAR	***FRR***	
Відбитки пальців	**2**	**3**	**3**	**2**	**10^{-4} %**	**0,6 %**	**$200**
Форма/геометрія долоні	2	2	2	3	10^{-3} %	0,1 %	$500
Розташування вен на тильній стороні долоні	2	3	3	1	10^{-4} %	0,5 %	$2000
Райдужна оболонка ока	3	3	3	2	10^{-9} %	0,05 %	$5000
Сітківка ока	3	3	2	1	10^{-5} %	0,08 %	$2000
Форма/геометрія обличчя (2D / 3D)	3	2	1	3	10^{-2} %	5 %	$1000
Термограма обличчя	3	3	1	3	10^{-3} %	0,8 %	$1500
Шкірне відображення	2	2	2	2	–	–	$1500
ДНК суб’єкта	3	3	3	1	–	–	$10000
Форма вух	2	2	2	2	–	–	–
Запах	2	2	2	1	–	–	–

Продовження таблиці 1.1

Властивість / **Біометрична характеристика**	***Універсальність***	***Унікальність***	***Незмінність***	***Вимірність***	***Надійність***		***Ціна***
					FAR	***FRR***	
Голос	2	1	1	2	10^{-2} %	3 %	$150
Рукописний почерк	1	1	1	3	–	–	–
Клавіатурний почерк	3	2	1	3	–	–	–
Хода	3	2	1	3	–	–	–
Рух губ	3	2	1	3	–	–	–

Як видно з таблиці, відбиток пальця, що є основною темою даної дисертації, має високу оцінку унікальності і постійності, і середню оцінку універсальності й вимірності. Дактилоскопічний метод має високу надійність – статистичні показники методу кращі за показники таких методів як аутентифікація за геометрією обличчя, голосом, підписом, клавіатурним подчерком. Також, досить низька вартість пристроїв, що сканують зображення відбитка пальця та досить проста процедура сканування відбитку.

З точки зору суб’єкта, біометрична ідентифікація є підготовчою операцією перед основними процедурами біометричної аутентифікації. Основним завданням біометричних систем є процедура біометричної аутентифікації. Принциповою відмінністю ідентифікації й аутентифікації є рівень довіри до суб’єкта. На попередньому етапі ідентифікації системи (навчання системи) рівень довіри до суб’єкта, який буде зареєстрований, апріорно високий. У багатокористувацькій системі біометрична ідентифікація обов'язково повинна проводитися під прямим контролем її власника або його представника, що підтверджує повноваження зареєстрованої особистості і коректність її поведінки при навчанні системи.

Режим біометричної аутентифікації, навпаки, передбачає високий рівень довіри до ідентифікованого суб'єкта. При біометричній аутентифікації суб'єкт повинен довести справжність свого заявленого імені шляхом пред'явлення своїх унікальних біометричних характеристик. Слід зазначити, що біометрична аутентифікація потенційно вразлива, якщо вона використовується незалежно від методів класичної аутентифікації, заснованих на протоколах з використанням паролів і ключів. Достатній рівень інформаційної безпеки може бути забезпечений лише шляхом поєднання методів класичної і біометричної аутентифікації.

Як видно з діаграми (Рис. – 1.5), дактилоскопічний метод, що заснований на унікальності візерунку папілярних ліній на пальцях людини, є найпоширенішим на сьогоднішній день біометричним методом.

Рисунок 1.5.1 – Розповсюдженість статичних біометричних методів, %

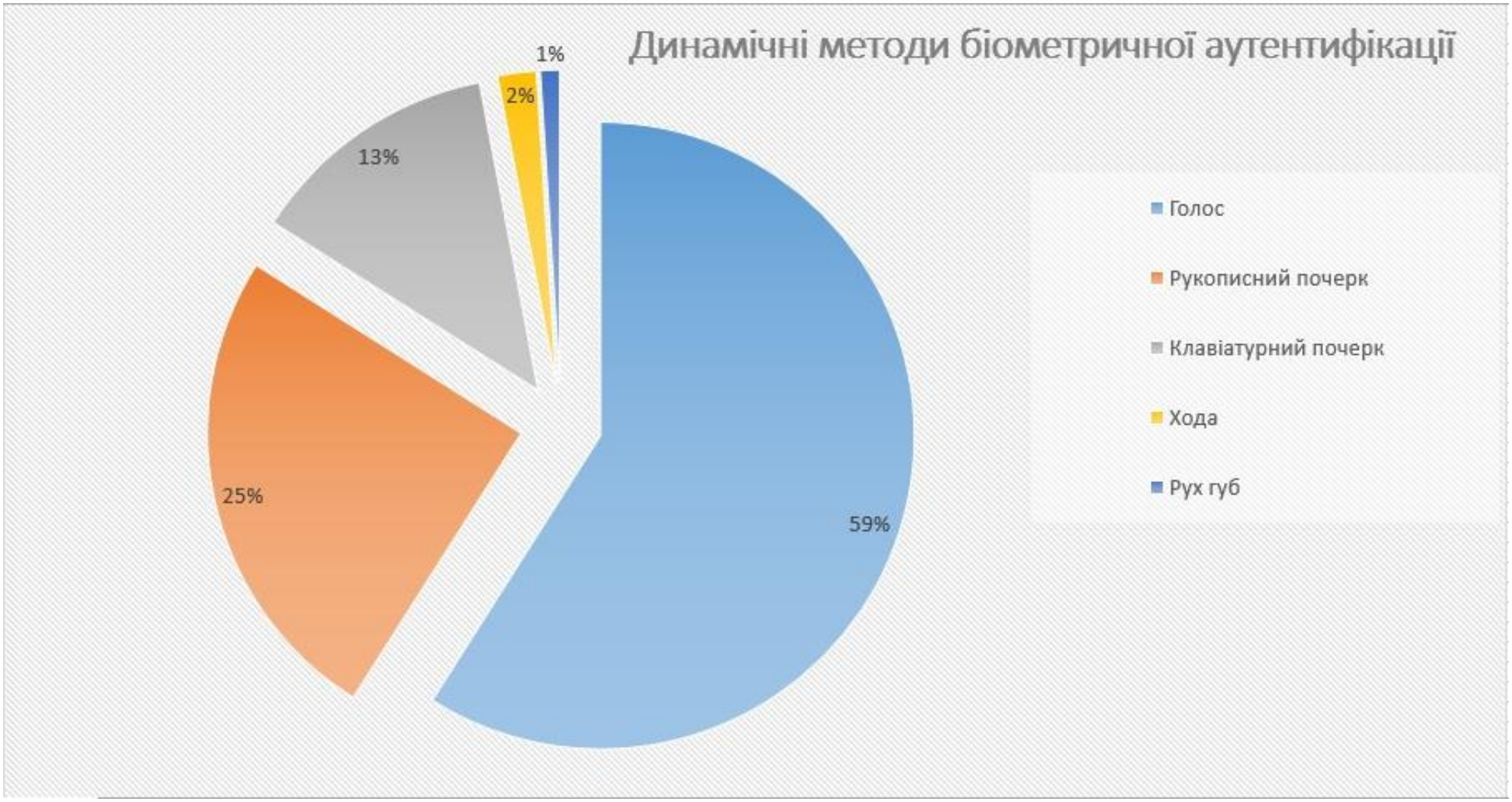

Рисунок 1.5.2 – Розповсюдженість динамічних біометричних методів, %

Висновки до розділу 1

У даному розділі були введені такі поняття як аутентифікація, біометрія, ідентифікація та верифікація. Були описані фактори аутентифікації, загальний принцип роботи біометричної системи та основні її характеристики. Також розглянуто основні методи біометричної аутентифікації, такі як статичні та динамічні.

На сьогоднішній день дактилоскопічний метод є найрозповсюдженішим методом аутентифікації та ідентифікації особи через його відносну дешевизну та високу ефективність, простоту у використані, легкість встановлення, компактність форми. Слід зауважити, що дактилоскопічна ідентифікація за застосовністю та доступністю з фінансової точки зору перевершує всі інші описані методи. Вона широко застосовується для аутентифікації з метою фізичного розмежування доступу або доступу до даних.

Тому саме дактилоскопічний метод біометричної аутентифікації буде розглянутий в наступних розділах, а також буде обрано найбільш ефективні алгоритми обробки зображення папілярного візерунку відбитку пальця.

2 КЛАСИФІКАЦІЯ БІОМЕТРИЧНИХ СИСТЕМ АУТЕНТИФІКАЦІЇ

Для реалізації деяких біометричних прикладних програм вимагається такий рівень технічних характеристик, який важко забезпечити за допомогою однієї біометричної характеристики. Такі прикладні програми дозволяють уникати використання декількох прикладних програм для перевірки документів, що підтверджують особу, а також для забезпечення безпеки при авіаперельотах. Крім того, такі прикладні програми необхідні для людей, котрі з тої чи іншої причини не можуть надати якісні біометричні зразки деяких біометричних модальностей.

Використання великої кількості біометричних характеристик, отриманих у результаті застосування декількох незалежних датчиків, алгоритмів або модальностей, як правило, забезпечує покращення технічних характеристик та зниження рівня ризику. Використання даних систем також забезпечує можливість прийняття рішення про допуск/недопуск суб’єкта при наявності будь-якого числа характеристик.

У даній роботі ми зосередимось на побудові мультиекземплярної біометричної системи, опираючись на правила, які регламентує міжнародний стандарт ISO/IEC 24722:2015.

2.1 Види біометричних систем

Поняття мультимодальний та мультибіометричний вказують на застосування більш ніж одного датчика, одного екземпляра та/або алгоритму в тій чи іншій комбінації для прийняття певного рішення щодо біометричної ідентифікації або верифікації. Метод об’єднання декількох зразків, ступенів схожості або рішень про схожість може бути елементарним або складним з математичної точки зору.

В мультибіометрії виділяють п’ять категорій біометричних систем:

- мультимодальна
- мультиалгоритмічна
- мультиекземплярна
- мультидатчикова
- мультипредставницька

Таблиця 2.1 – Категорії мультибіометричних систем

Категорія	**Модальність**	**Алгоритм**	**Біометрична характеристика**	**Датчик**
Мультимодальна	**2 (завжди)**	2 (завжди)	2 (завжди)	2 (зазвичай)
Мультиалгоритмічна	1 (завжди)	**2 (завжди)**	1 (завжди)	1 (завжди)
Мультиекземплярна	1 (завжди)	1 (завжди)	**2 екземпляри однієї характеристики (завжди)**	1 (зазвичай)
Мультидатчикова	1 (завжди)	1 (зазвичай)	1 (завжди, той самий екземпляр)	**2 (завжди)**
Мультипредставницька	1	1	1	1

2.2 Мономодальна біометрична система

Стандартна мономодальна система будується за наступною схемою:

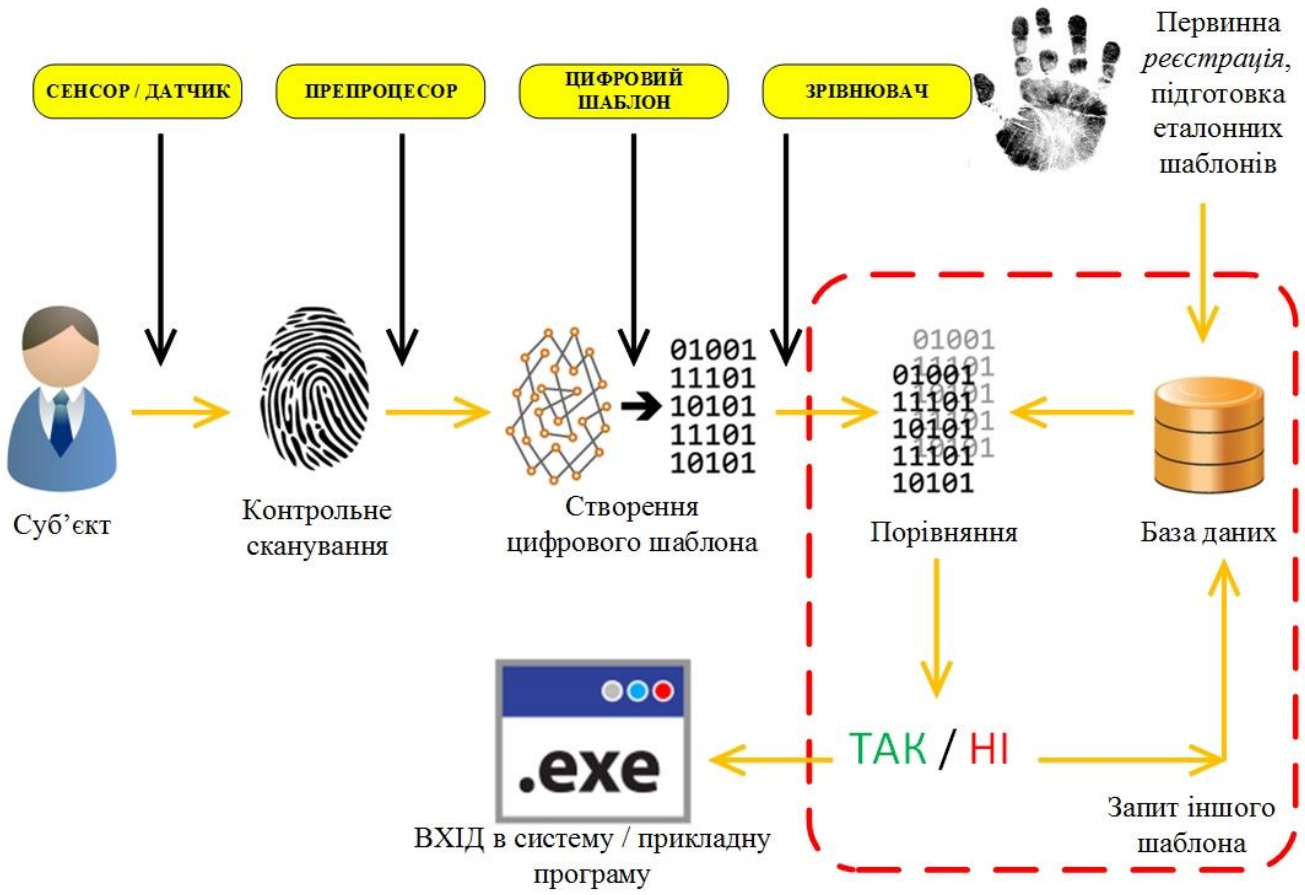

Рисунок 2.1 – Схема роботи мономодальної біометричної системи

Перше приватне й індивідуальне застосування біометричної системи називається – *реєстрація*. У процесі реєстрації біометрична інформація від суб'єкта зберігається у базі даних – це база шаблонів зареєстрованих суб'єктів. Надалі біометрична інформація реєструється і порівнюється з інформацією, отриманою раніше. Якщо необхідно, щоб біометрична система була надійна, дуже важливо, щоб зберігання і пошук всередині самих систем були безпечними.

Біометрична ознака потрапляє на *сенсор* або *сканер* – це проміжний зв'язок між реальним світом і системою; він повинен отримати всі необхідні дані. У більшості випадків це зображення, але сенсор може працювати і з іншими даними відповідно до бажаних характеристик [2].

Наступний блок – *препроцесор* – здійснює всі необхідні попередні процеси: він повинен видалити все «зайве» з сенсора для збільшення чутливості на вході (наприклад, видалення фонових шумів при розпізнаванні голосу).

В наступному блоці створюється *цифровий шаблон*. Шаблон – це синтез (сукупність) релевантних характеристик, зазвичай, представляє собою компактну структуру даних, яка відображає характерні ознаки відбитка, і зручна для порівняння. Елементи біометричного вимірювання, які не використовуються в порівняльному алгоритмі, не зберігаються в шаблоні, щоб зменшити розмір файлу і захистити особистість зареєстрованого, унеможлививши відтворення вихідних даних за інформацією з шаблону.

З бази даних обирається шаблон еталонного відбитка, передається до *зрівнювача* (будь-якого алгоритму порівняння), і між ним і даним відбитком обчислюється *оцінка схожості* (наприклад, англ. Hamming distance – відстань Хеммінга – число позицій цифр у двох, однакової довжини, кодових посилках (надісланій та отриманій), в яких відповідні цифри відрізняються). Дана оцінка порівнюється з деяким *граничним значенням*, і приймається рішення про ідентичність отриманого відбитка і еталонного.

2.3 Мультимодальна біометрична система

Для підвищення точності застосовуються мультимодальні системи. Мультимодальні системи приймають вхідний сигнал із одного або багатьох датчиків, котрі отримують біометричні характеристики від двох або більше модальностей. Наприклад, одна система, яка комбінує інформацію за геометрією обличчя та райдужною оболонкою ока для біометричного розпізнавання, розглядається як мультимодальная система незалежно від того, чи різними пристроями були отримані зображення обличчя та райдужної оболонки ока, чи одним і тим же. Такою не вимагається, щоб різні виміри були об'єднані математично. Наприклад, система з аутентифікацією за відбитками пальців і за голосом буде вважатися мультимодальной навіть при використанні алгоритму «АБО», що дозволяє розпізнавати суб’єкта за допомогою тієї чи іншої модальності [13].

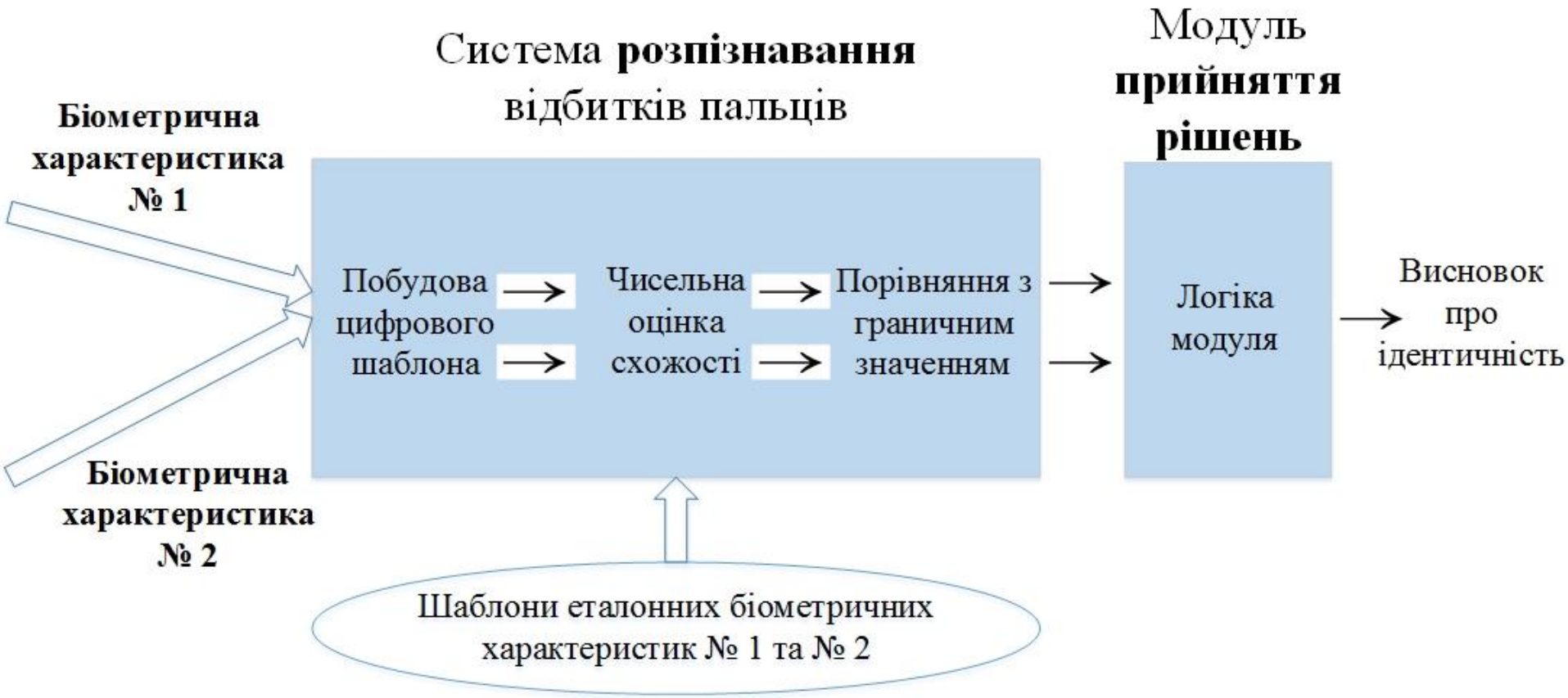

Рисунок 2.2 – Схема роботи мультимодальної біометричної системи, яка використовує 2 біометричні характеристики

2.4 Мультиалгоритмічна біометрична система

Мультиалгоритмічні біометричні системи отримують один шаблон із одного датчика й обробляють даний шаблон за допомогою двох і більше алгоритмів. Даний метод може бути застосований до будь-якої модальності. Максимальний ефект може бути досягнутий при застосуванні алгоритмів, заснованих на різних незалежних принципах (такі алгоритми називають – *ортогональними*).

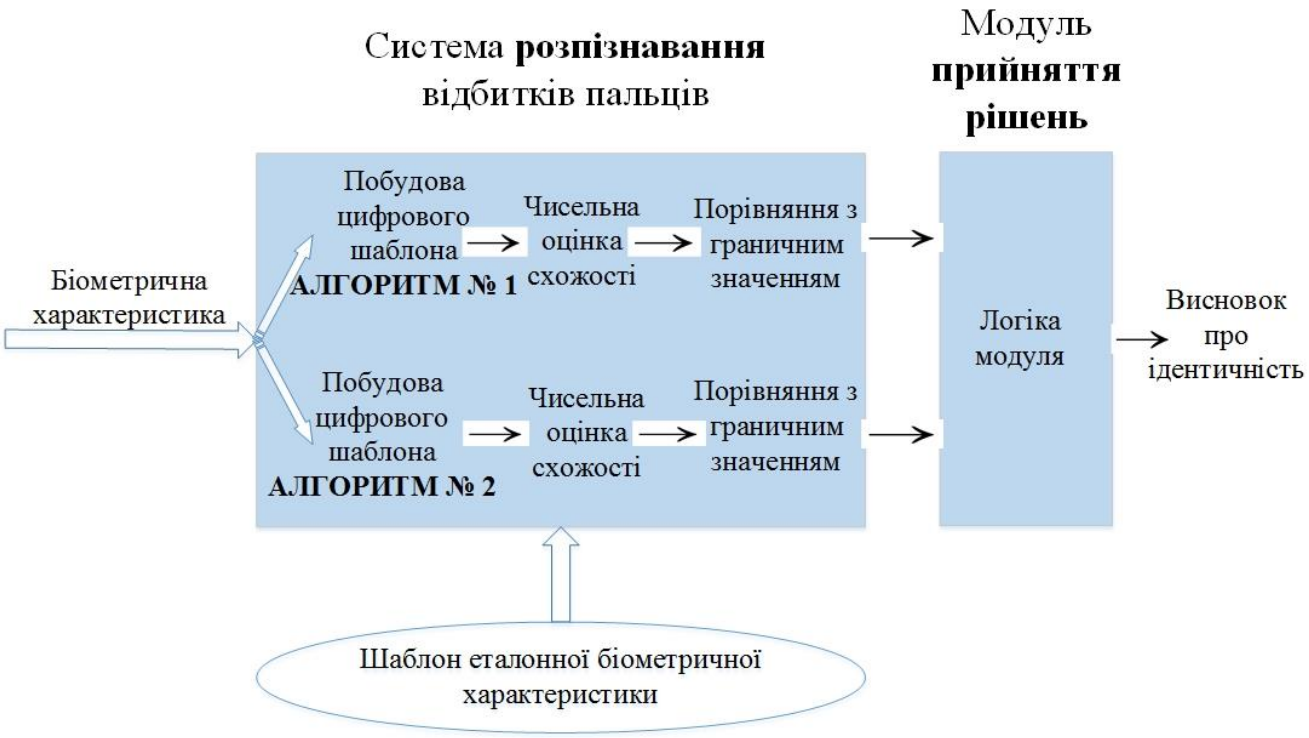

Рисунок 2.3 – Схема роботи мультиалгоритмічної біометричної системи, яка використовує 2 алгоритми побудови шаблонів

2.5 Мультиекземплярна біометрична система

Мультиекземплярні біометричні системи застосовують один (або декілька) датчик(ів) для отримання шаблонів двох або більше різних екземплярів однієї й тієї ж біометричної характеристики. Наприклад, системи, які отримують зображення декількох відбитків пальців, вважають мультиекземплярними, а не мультимодальними. Однак системи, які отримують, наприклад, послідовні кадри зображень обличчя або райдужної оболонки ока, розглядаються як системи мультипредставлення, а не мультиекземплярні.

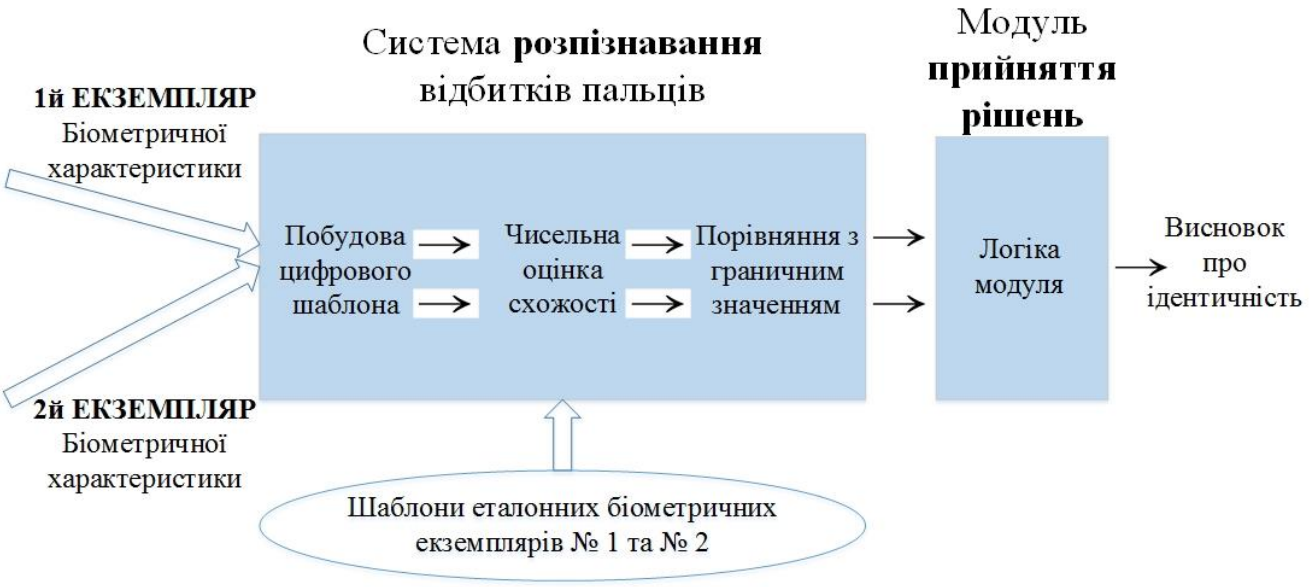

Рисунок 2.4 – Схема роботи мультиекземплярної біометричної системи, яка використовує 2 екземпляри однієї і тієї ж біометричної характеристики

2.6 Мультидатчикова біометрична система

Мультидатчикові біометричні системи отримують один і той же екземпляр біометричної характеристики за допомогою двох або більше різних датчиків. Обробку декількох шаблонів проводять за допомогою одного алгоритму або комбінації декількох алгоритмів. Наприклад, для розпізнавання геометрії обличчя можна використовувати як камеру, що працює у видимому діапазоні, так і інфрачервону камеру, що працює на певній довжині(ах) хвилі(хвиль) інфрачервоного випромінювання.

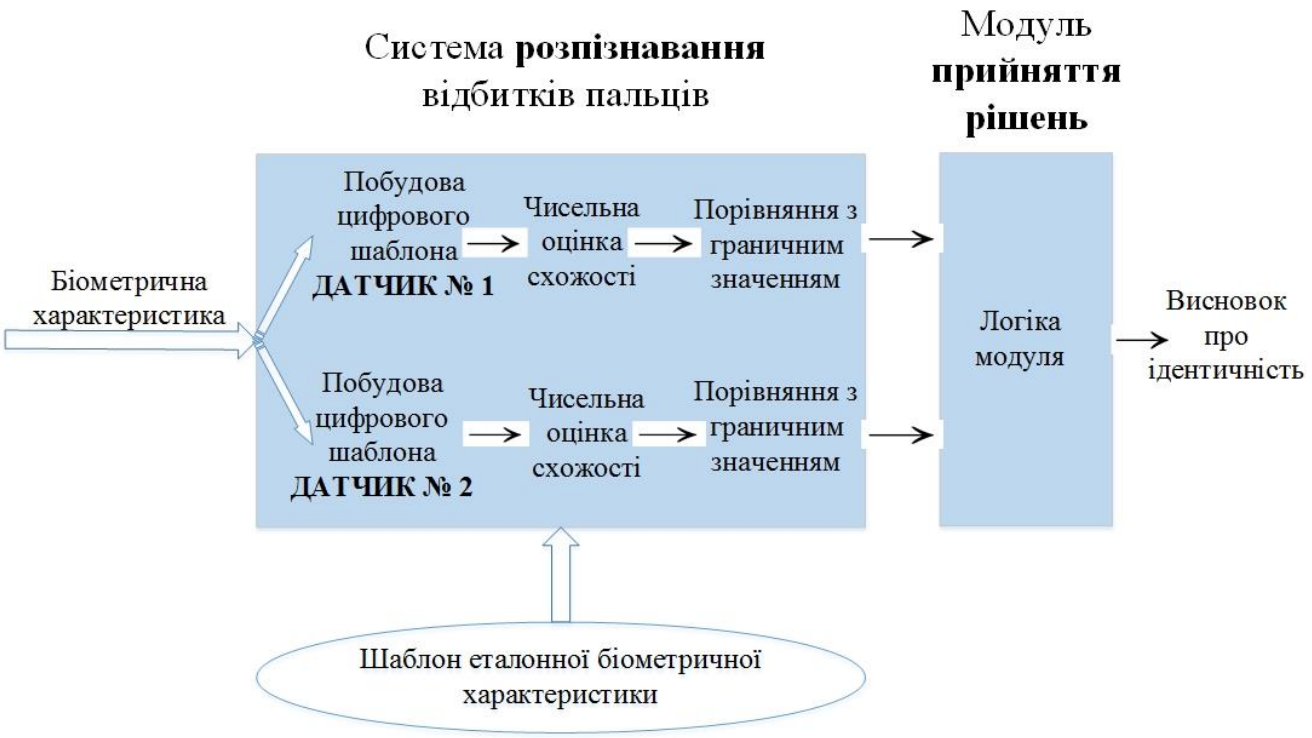

Рисунок 2.5 – Схема роботи мультидатчикової біометричної системи, яка використовує 3 датчики для сканування біометричної характеристики

2.7 Мультипредставницька біометрична система

Мультипредставницькі біометричні системи використовують кілька представлень шаблонів одного екземпляра біометричної характеристики або єдиного представлення, що є результатом отримання декількох шаблонів. Наприклад, кілька кадрів зображення обличчя, зроблених відеокамерою, але не обов'язково послідовних.

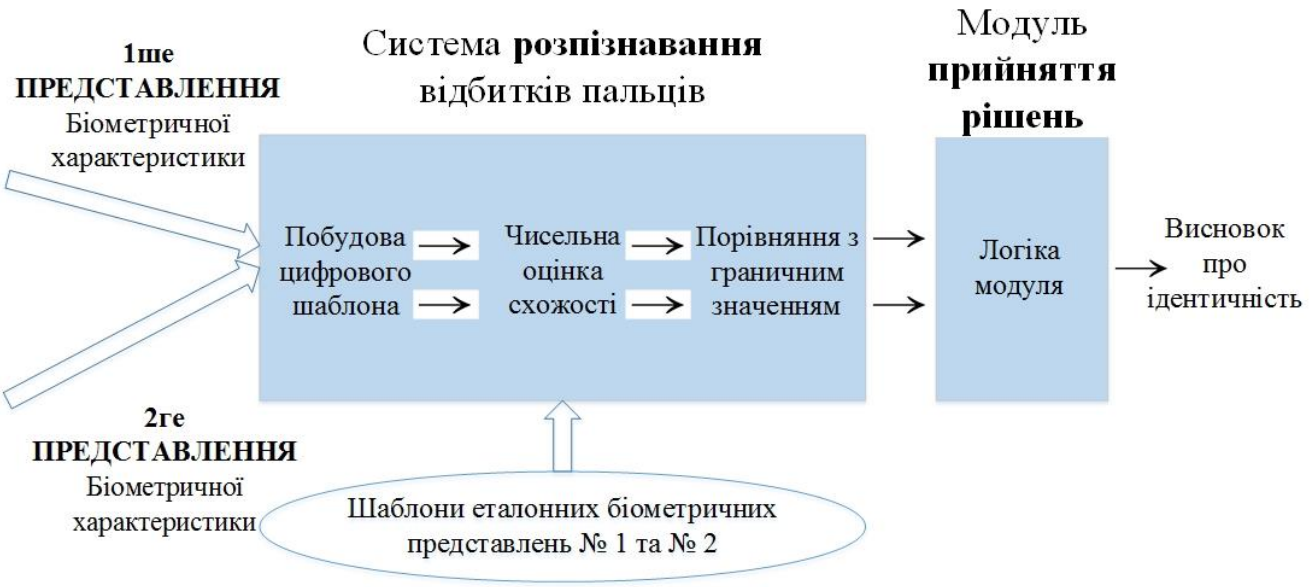

Рисунок 2.6 – Схема роботи мультипредставницької біометричної системи, яка використовує 3 представлення біометричної характеристики

Висновки до розділу 2

У даному розділі розглянуто основні системи біометричної аутентифікації, був описаний загальний алгоритм роботи систем біометричної аутентифікації.

Проведений аналіз показує, що при збільшенні кількості модальностей виникає проблема прийняття рішення. У випадку з кількома модулями і, відповідно, декількома відповідями є наступні стратегії прийняття рішень.

- Порівняння за граничним значенням і винесення позитивного рішення, якщо всі модулі відповіли позитивно. Цей випадок характеризується меншою ймовірністю помилкового допуску і більшою – помилкою відмови в допуску.
- Порівняння за граничним значенням і голосування простою більшістю. Цей випадок, навпаки, підвищує ймовірність помилкового допуску і знижує – помилку відмови в допуску.
- Висновок рішення за допомогою нечіткої логіки. Цей спосіб дозволяє детально налаштувати процес прийняття рішення і дає можливість враховувати більшу кількість факторів.

Поняття нечіткої логіки та її основ буде докладніше описано у наступному розділі, а також буде побудована мультиекземплярна біометрична система відбитків пальців із підсистемою прийняття рішень на основі правил нечіткої логіки.

3 ПОБУДОВА БІОМЕТРИЧНОЇ СИСТЕМИ ДЛЯ РОЗПІЗНАННЯ ВІДБИТКІВ ПАЛЬЦІВ

3.1 Нечітка логіка

Нечітка логіка узагальнює теорію множин і класичну логіку. Поняття нечіткої множини введено вперше Лотфі Заде в 1965 році. Нечітка множина **A** – це сукупність упорядкованих пар, складених з елементів **x** універсальної множини **X** і відповідних ступенів належності $\mu_A(x)$ [6].

$$A = \left\{ \left(x, \mu_A(x) \right) \middle| x \in X \right\}$$

Функція приналежності $\mu_A(x)$ вказує, якою мірою елемент **x** належить множині **A**. Множина значень цієї функції – інтервал [0, 1]. У разі множини значень {0, 1}, нечітка множина є звичайною множиною [7].

На відміну від класичних множин над нечіткими множинами, операції об'єднання і перетину визначаються трьома різними способами:

- Максимінні

$$\mu_{A \cup B}(x) = \min\left(\mu_A(x), \mu_B(x) \right)$$

$$\mu_{A \cap B}(x) = \max\left(\mu_A(x), \mu_B(x) \right)$$

- Алгебраїчні

$$\mu_{A \cup B}(x) = \mu_A(x) + \mu_B(x) - \mu_A(x) * \mu_B(x)$$

$$\mu_{A \cup B}(x) = \mu_A(x) + \mu_B(x) - \mu_A(x) * \mu_B(x)$$

- Обмежуючі

$$\mu_{A \cup B}(x) = \min\left(1, \mu_A(x) + \mu_B(x) \right)$$

$$\mu_{A \cap B}(x) = \min\left(0, \mu_A(x) + \mu_B(x) - 1 \right)$$

Висновок в нечіткій логіці ґрунтується на лінгвістичних змінних [5]. Це змінні, значеннями яких є фрази деякої мови. Наприклад, змінна "Якість" може приймати значення "Висока", "Середня", "Низька". Кожне значення лінгвістичної

змінної є нечіткою множиною. Наприклад, Якість може бути Високою на 0,8 і Низькою на 0,1.

Висновок проходить в три етапи.

- фазифікації (fuzzification)

Чисельні значення переводяться в значення лінгвістичних змінних за допомогою застосування відповідних функцій приналежності.

- застосування правил

Правила мають стандартний вигляд "якщо А, то В" і використовують лінгвістичні змінні. Спочатку обчислюється ступінь приналежності посилки. Для цього використовується один з трьох видів операцій над множинами. Після цього значенню змінної у кінцевому випадку присвоюється обчислений ступінь приналежності.

- дефазифікація (defuzzification)

З виведених змінних отримують чисельні значення і результати.

3.2 Нечітка логіка в біометричних системах

На жаль, застосування нечіткої логіки в біометричних системах слабо представлено в поточних дослідженнях.

У статті Fuzzy Fusion in Multimodal Biometric Systems [9] професор V.Conti зі співавторами описує мультимодальну біометричну систему для розпізнавання відбитків пальців, що використовує відбитки вказівного та середнього пальця. Як додаткові фактори при прийнятті рішення про ідентичність, використовується якість відбитку пальця. Проте відсутність правил виведення нечіткої логіки та опису методів оцінки якості роблять результати неверифікованими.

Стаття Fuzzy Logic Decision Fusion in a Multimodal Biometric System [8] описує мультимодальну біометричну систему, в якій використовується запис голосу, фотографія обличчя та відбиток пальця. Нечітка логіка в ній

використовується не безпосередньо для прийняття рішення, а для обчислення коефіцієнтів, з якими використовується міра схожості відбитків та фотографій.

У даній роботі була розроблена мультимодальна біометрична система з нечітким висновком, що використовує три відбитки пальця, де якість відбитку оцінювалась декількома різними алгоритмами, у тому числі і стандартним NFIQ, в якій були враховані недоліки робіт [8] і [9].

3.3 Побудова мультиекземплярної біометричної системи

Для реалізації мультиекземплярної біометричної системи була обрана система, що працює з трьома відбитками пальців. З біометричних ознак обрані відбитки пальців, оскільки вони прості у використанні і дають надійні результати. В системі використовуються саме три відбитки, так як менша кількість біометричних ознак не дає повною мірою можливості відчувати різні стратегії прийняття рішення, більша ж кількість уповільнює роботу системи, але не дає змістовної відмінності від трьох відбитків.

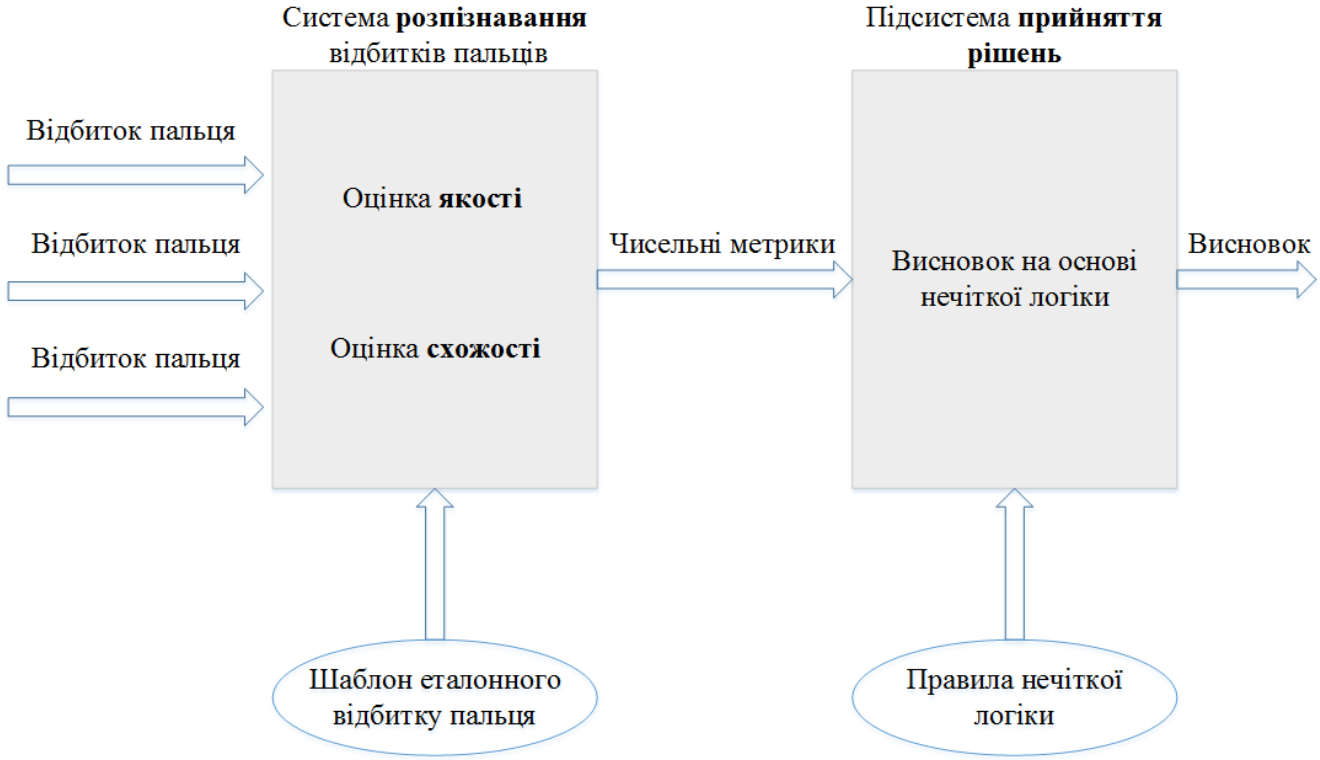

Рисунок 3.3 – Архітектура мультиекземплярної біометричної системи

Вся система складається з двох основних частин: системи розпізнавання відбитків пальців і підсистеми прийняття рішення. Система розпізнавання складається з незалежних модулів: модуля оцінки схожості двох відбитків і модуля оцінки якості початкового відбитка.

3.4 Вимірювання якості відбитків пальців

Відбитки пальців, як унікальні та незмінні характеристики людини, широко використовуються для ідентифікації особи. Так чи інакше, для алгоритмів розпізнавання і співставлення відбитків важлива якість зображень, наприклад, відсутність шуму. Під шумом маються на увазі змащені області відбитка, області без вираженого спрямування папілярних ліній і т.д., із яких неможливо отримати інформацію, що характеризує відбиток.

Причини отримання неякісних зображень відбитків можуть бути різні: занадто жирна або суха шкіра рук, великі пори або випадковий рух пальця при знятті відбитків (див. Рис. 3.4.1).

Рисунок 3.4.1 – Приклади відбитків пальців

Неякісні зображення відбитків пальців, як правило, характеризуються відсутністю виражених напрямків папілярних ліній і низькою контрастністю.

На даний момент існують два основних алгоритми визначення якості відбитків: NFIQ (NIST Fingerprint Image Quality) та LFIQ (Latent Fingerprint Image Quality). Останній є досить специфічним, так як використовується для відбитків, знайдених на місці злочину. Тому в роботі буде розглянуто алгоритм NFIQ [10].

Для отримання більш точної оцінки якості застосовуються три алгоритми, які вимірюють якість відбитка пальця за різними критеріями.

3.4.1 Алгоритм NFIQ – NIST Fingerprint Image Quality

NFIQ (NIST Fingerprint Image Quality) – це алгоритм визначення якості відбитків пальців, розроблений у Національному Інституті стандартів та технологій (NIST). Для оцінки якості використовується інформація про напрямки та кривизну папілярних ліній, про контрастність зображення [16].

На вхід алгоритму подається зображення в градаціях сірого, яке розбивається на непересічні блоки. Для кожного блоку визначено вікно – область, що використовується для отримання інформації щодо якості блоку, яка включає в себе сам блок і деяке його оточення. Вікна можуть між собою перетинатися.

Далі для кожного блоку обчислюється напрямок, визначається ступінь кривизни папілярних ліній, ступінь контрастності зображення. За цими характеристиками обчислюється значення якості блока. Існує п’ять рівнів якості: погана (5), середня (4), добра (3), дуже добра (2) і відмінна (1). Значення якості для кожного блоку відбитка утворюють карту якості. На підставі даної карти обчислюється характеристичний вектор і статистика якості мінуцій відбитку, де під якістю мінуції мається на увазі якість блока, в якому вона знаходиться. Потім характеристичний вектор використовується як вхід для багатошарового перцептрона (MLP), що є класифікатором.

На виході алгоритм видає значення якості всього зображення відбитка пальця, аналогічно випадку з окремими блоками.

В алгоритмі NFIQ якість відбитка визначається в залежності від контрастності зображення, визначення напрямку папілярних ліній і областей високої кривизни. Так для кожного відбитка обчислюються:

- карта напрямків;
- карта низького контрасту;
- карта невизначеного напрямку;
- карта високої кривизни.

Мета створення даної карти – показати області з достатньою кількістю ребер та виявити їхній загальний напрямок.

Спочатку зображення ділиться на непересічні квадратні блоки зі стороною M=8 (см. Рис. 5). Для визначення загального напрямку блока потрібно розглянути деяке оточення – вікно зі стороною L=24 зміщення блоку щодо вікна N=8). Якщо розмір зображення не кратний розміру блоку, вікно може зайти за межі зображення. У цьому випадку зображення доповнюється середніми значеннями сірого – 128.

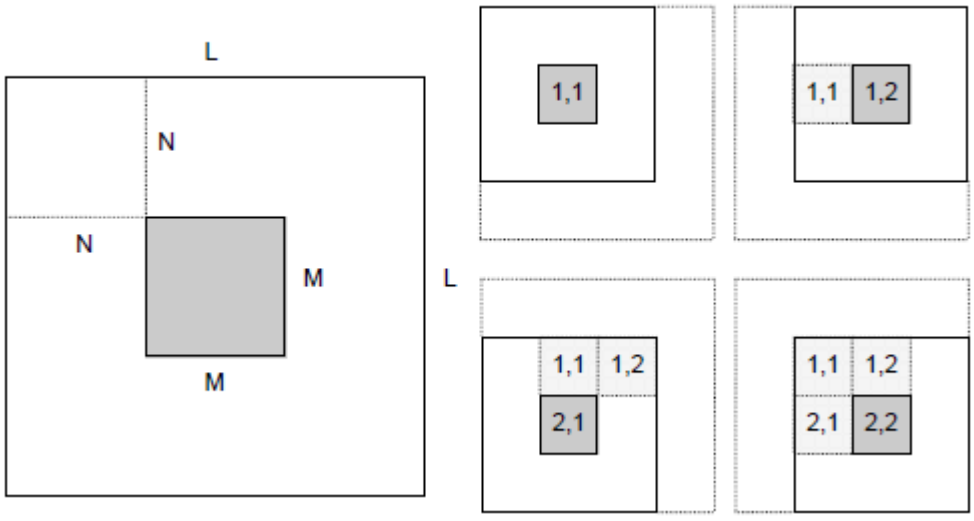

Рисунок 3.4.2 – Блоки зображення і ті, що перекриваються вікнами

Далі для кожного блоку зображення ми інкрементально повертаємо його вікно відповідно до кожного із 16 напрямків (кут між напрямками дорівнює 11.25°) і проводимо DFT (дискретне перетворення Фур'є) для кожного напрямку, тобто повороту вікна. Так кожному напрямку відповідає число від 0 до 15, а блокам без визначеного напрямку відповідає -1.

Приклад визначених напрямків представлено на Рисунку 3.4.3, а на Рисунку 3.4.3 – карта напрямків.

Рисунок 3.4.3 – Частина оригінального зображення відбитку пальця і це ж зображення з виділеними напрямками

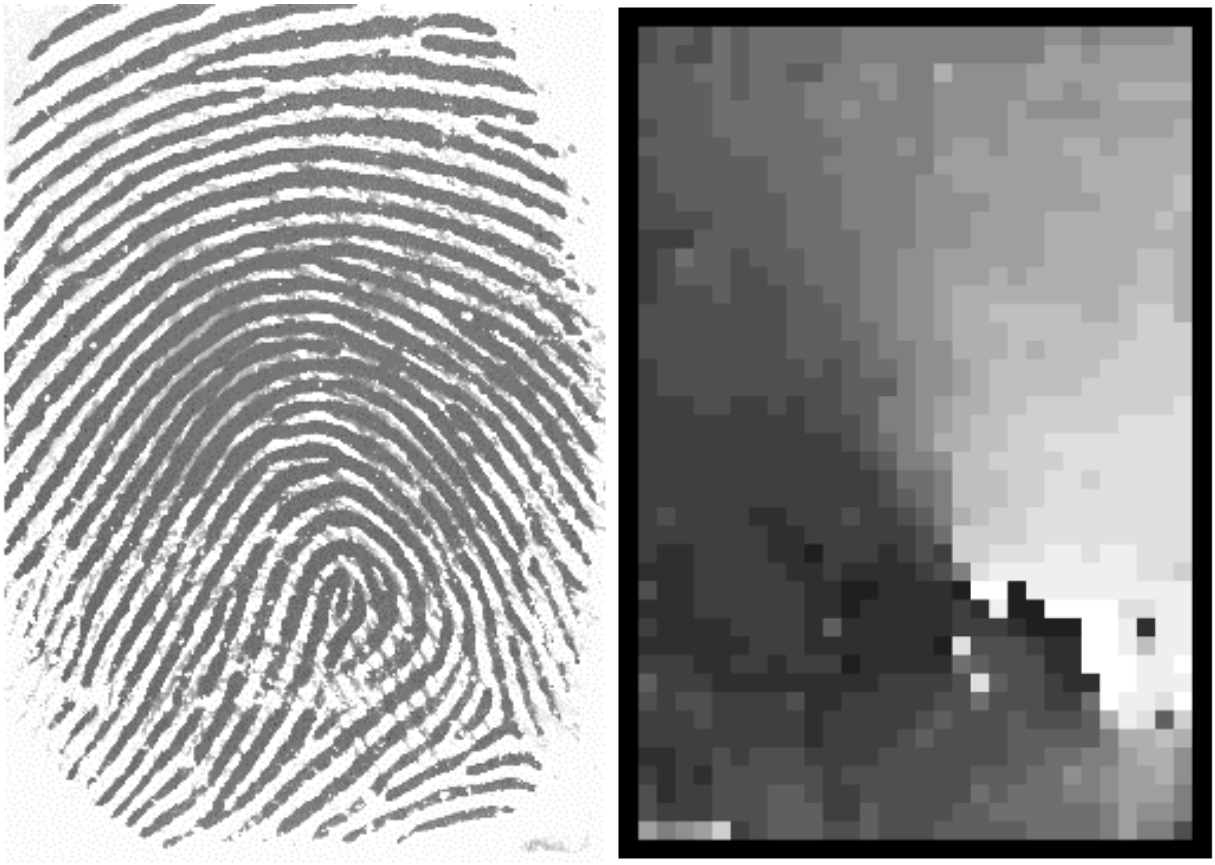

Рисунок 3.4.4 – Зображення відбитку пальця і його карта напрямків

Об’єднуючи всі описані вище результати, обчислюється карта якості відбитку. Кожному блоку зображення присвоюється значення від 5 (погана якість) до 1 (відмінна якість). На Рисунку 3.4.5 показано приклад карти якості. Області якості 1 позначені білим кольором, а області якості 5 – чорним.

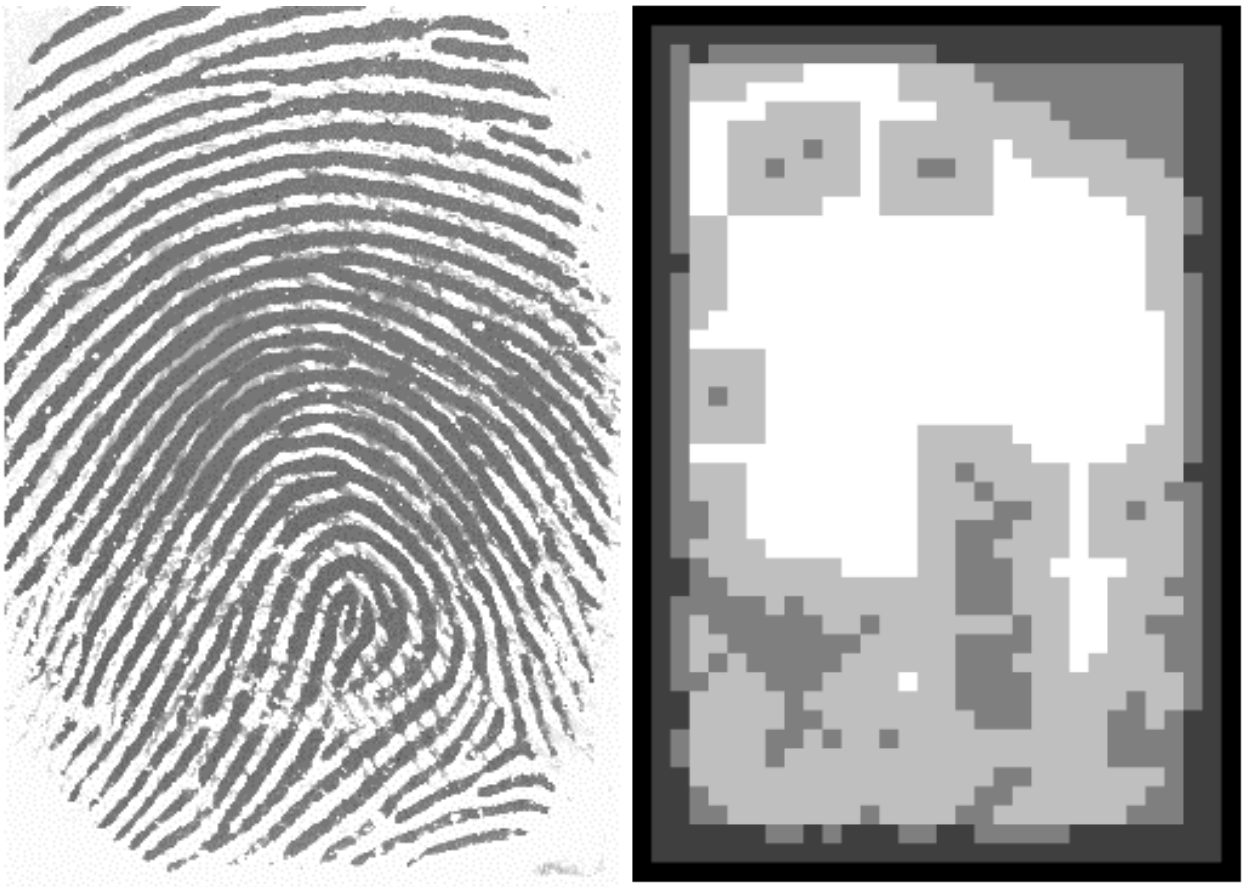

Рисунок 3.4.5 – Відбиток пальця та його карта якості

В алгоритмі NFIQ визначалась якість всього зображення відбитка. Проте, як правило, у кожного зображення є якісні області, за якими відбиток може бути ідентифіковано. Якщо відсоток таких областей невеликий, то зображення в цілому буде оцінено як неякісне, навіть якщо у них міститься достатньо достовірної інформації.

Для того, щоб була можливість використовувати зображення відбитків у таких ситуаціях, було прийнято рішення використовувати для співставлення лише якісні області відбитків, тобто блоки якості 1, 2, 3. Таким чином, будуть отримані достовірні результати навіть для тих відбитків, які можуть бути визнані неякісними.

Алгоритм NFIQ – NIST Fingerprint Image Quality є стандартним і широко використовуваним алгоритмом для оцінки якості відбитків пальців. Він розроблений в Національному Інституті Стандартів і Технологій. При оцінці

якості він враховує напрямок папілярних ліній, контраст відбитка і кривизну папілярних ліній. Зображення розбивається на блоки і якість оцінюється незалежно в кожному блоці. На виході алгоритму виходить карта якості, яка містить оцінку від 1 до 5 для кожного блока відбитка. З неї можна отримати дві чисельні оцінки - відсоток блоків низької якості і середню якість всього відбитка.

3.4.2 Виділення фону

Виділення фону – частини зображення без папілярних ліній. Даний алгоритм заснований на порівнянні визначеності напрямку (того, наскільки виражені папілярні лінії) в даному блоці і в середньому по всьому відбитку. На виході алгоритму виходить метрика, що показує відсоток фону на всьому зображенні [12].

Рисунок 3.4.6 – Відбиток пальця з великою кількістю фону

3.4.3 Оцінка яскравості

Оцінка яскравості – відбитки з низькою яскравістю виходять, якщо палець, який сканують, був занадто вологим. Це призводить до того, що папілярні лінії зливаються разом. На відміну від темних, світлі відбитки, зазвичай, не є неякісними, і на них читаються папілярні лінії. Оцінка будується підрахунком тих пікселів, чия яскравість нижче певного порогу. Процентне співвідношення таких пікселів до всіх пікселів відбитка визначає метрику якості [12].

Рисунок 3.4.7 – Відбиток пальця з папілярними лініями, що зливаються

Визначення яскравості і фону доповнюють оцінку якості NFIQ, так як в ньому ці параметри не враховуються.

Параметри методів визначення якості відбитків були підібрані емпірично. Таким чином, були визначені граничні значення яскравості пікселів, які вважалися темними, коефіцієнт порівняння визначеності напрямку при оцінці фону та інші параметри.

3.5 Оцінка схожості двох відбитків

Другий модуль системи розпізнавання відбитків оцінює те, з якою ймовірністю два відбитка пальця є відбитками одного і того ж пальця людини.

Перед визначенням схожості проводиться поліпшення якості зображення відбитка пальця і приведення його до вигляду, зручного для подальшої роботи.

Порівняння за особливими точками – за одним чи декількома зображеннями відбитків пальців зі сканера формується шаблон (карта), що являє собою двомірну поверхню, на якій виділені кінцеві точки і точки розгалуження. Процедура порівняння полягає в тому, що на відсканованому зображенні відбитку також виділяються особливі точки, складається тимчасова карта цих точок, яка порівнюється з шаблоном, і за кількістю точок, що збіглися, приймається рішення за ідентичністю відбитків. Результатом співставлення, як правило, є набір ключових точок. Потім використовується поріг, який визначає, наскільки великим повинно бути це число, щоб було можливо зіставити відбиток пальця з шаблоном. У роботі алгоритмів даного класу реалізуються механізми кореляційного порівняння, але при порівнянні положення кожної з імовірно відповідних одна одній точок [4].

Розглянемо етапи порівняння двох відбитків за локальними ознаками:

Етап 1: Покращення якості вихідного зображення відбитку. Збільшується різкість меж папілярних ліній.

Етап 2: Сегментація – обчислення поля орієнтації папілярних ліній відбитку. Зображення розбивається на квадратні блоки, зі стороною більше 4

пікселів і за градієнтами яскравості обчислюється кут θ орієнтації ліній для фрагмента відбитку.

Етап 3: Бінаризація зображення відбитку. Зведення до чорно-білого зображення (1 bit) пороговою обробкою.

Етап 4: Потоншення ліній зображення відбитку. Потоншення проводиться до тих пір, поки лінії не будуть шириною 1 піксель.

Етап 5: Вилучення мінуцій. Зображення розбивається на блоки 9x9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центра. Піксель у центрі вважається мінуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів: один (мінуція - «закінчення») чи два (мінуція - «роздвоєння») чи три (мінуція «розгалуження»).

Координати виявлених деталей та їх кути орієнтації записуються у вектор: $W(p)=[(x_1, y_1, \theta_1), (x_2, y_2, \theta_2)\ldots(x_p, y_p, \theta_p)]$, де p – число мінуцій. При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнанні вектор визначає поточний відбиток (що досить логічно).

Етап 6: Співставлення мінуцій. Два відбитки одного пальця будуть відрізнятися один від одного поворотом, зміщенням, зміною масштабу і площею дотику в залежності від того, як користувач прикладає палець до сканеру. Тому не можна сказати, чи належить відбиток людині, чи ні на підставі простого їхнього порівняння (вектори еталону і поточного відбитку можуть відрізнятися за довжиною, містити невідповідні деталі тощо). Через це процес зіставлення повинен бути реалізованим для кожної деталі окремо.

Етапи порівняння:

- Реєстрація даних. Визначаються параметри афінних перетворень (кут повороту, масштаб і здвиг), при яких деяка деталь із одного вектору відповідає деякій деталі з іншого;
- Пошук пар відповідних деталей. При пошуку для кожної деталі потрібно перебрати до 30 значень повороту (від -15 градусів до +15), 500 значень здвигу (від -250 пікселів до +250 пікселів - хоча, звичайно, межі обирають і поменше) і 10 значень масштабу (від 0,5 до 1,5 з

кроком 0,1). Всього до 150 000 кроків для кожної із 70 можливих деталей. На практиці, всі можливі варіанти не перебираються – після підбору потрібних значень для однієї деталі їх же намагаються підставити і до інших деталей, інакше було б можливо зіставити практично будь-які відбитки один одному;

- Оцінка відповідності відбитків. Оцінка відповідності відбитків виконується за формулою:

$$K = \frac{D^2}{p \cdot q} \times 100\%$$

де D – кількість мінуцій, що збіглися, p – кількість мінуцій еталона, q – кількість мінуцій відбитку, що ідентифікується).

У разі, якщо результат перевищує 65%, відбитки вважаються ідентичними (поріг може бути знижений виставлянням іншого рівня пильності).

Якщо виконувалася аутентифікація, то на цьому все і закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків, що знаходяться в базі даних. Потім вибирається користувач, у якого найбільший рівень відповідності (зрозуміло, його результат повинен бути вище порога 65%) [4].

Головною перевагою алгоритму порівняння відбитків пальців за особливими точками є швидкість його роботи. Найбільше часу в процесі ідентифікації займає перебір еталонів в пошуку відбитка, ідентичного тимчасовому. Однак набагато простіше і швидше порівняти кілька десятків окремих точок, ніж ціле зображення. Тим більше, що в цьому випадку використовуються спеціальні алгоритми кореляційного порівняння. Вони враховують положення імовірно співпадаючих точок для обертання або зсуву тимчасової карти. А це дозволяє ще більше прискорити процес ідентифікації. До переваг можна також віднести те, що метод є широко відомим і добре дослідженим, використовується в додатках AFIS, а також підходить для множинного зіставлення. Тому в силу простоти реалізації і швидкості роботи – алгоритми даного класу є найбільш поширеними.

До недоліків слід віднести високі вимоги до якості зображення папілярного візерунку (дозволу) і розміру чутливого датчика. Для їх задоволення сканер повинен забезпечувати дозвіл не менше 300, а краще – близько 500 dpi. При використанні сканерів, менш специфічних, ніж AFIS, дає низькі результати. Також слід враховувати, що люди, які не мають зовсім, або мають невелику кількість ключових точок (особливий стан шкіряного покриву) не можуть користуватися даною системою. Кількість ключових точок може бути обмежуючим фактором для безпеки алгоритму. Крім того, можливі збої в системі через хибні ключові точки (ділянка, що містить помилку, яка виникла через низьку якість реєстрації, відтворення зображення або нечіткого відбитку смуг) [4].

3.5.1 Виділення мінуцій – алгоритм MCC (Minutia Cylinder Code)

Після поліпшення зображення проводиться виділення мінуцій. Мінуція – це особлива точка на відбитку пальця, на якій папілярна лінія роздвоюється або закінчується. Саме взаємне розташування мінуцій і їх вид є унікальним для кожної людини.

Далі за набором мінуцій будується шаблон – компактна структура даних, зручна для порівняння.

Одним із найсучасніших алгоритмів локального зіставлення є алгоритм MCC (Minutiae Cylinder-Codes) [14]. MCC розроблений в Лабораторії біометричних систем Болонського університету. Даний алгоритм стійкий до поворотів відбитка, його зрушень і розтягування.

Першим кроком алгоритму є побудова структури даних, яка називається циліндром, для кожної мінуції шаблону. Циліндр – це лінеаризоване представлення тривимірного кубоїда, у якого дві координати відповідають різниці в координатах щодо вихідної мінуції, а третя – дискретизованій різниці у напрямках. Значення клітинок кубоїда складаються із суми метрики за кожною із

мінуцій – мінуція має тим більшу метрику, чим ближче різниця її координат і напрямку щодо вихідної до координат клітинки. Зіставлення циліндрів здійснюється шляхом представлення значень клітинок як координат у багатовимірному просторі та обчислення евклідової відстані. Циліндри можуть бути також бінаризованими шляхом порівняння значень клітинок з порогом, що дозволяє використовувати ефективні бітові обчислення. Результатом зіставлення окремих циліндрів є матриця індивідуальних зіставлень, яка є основою для кроку об'єднання. Об'єднання відбувається шляхом визначення середньої схожості кращих зіставлень з повторами циліндрів або без повторів, в останньому випадку для визначення кращих зіставлень використовується угорський алгоритм. Для більш точних результатів до матриці може застосовуватися процедура релаксації.

Мірою схожості двох відбитків виступає сума відстаней Хеммінга між "циліндрами".

Висновки до розділу 3

У даному розділі були введені основні поняття та принципи нечіткої логіки, представлений метод, за яким буде в подальшому проводитися навчання біометричної системи. Була побудована сама мультиекземплярна біометрична система відбитків пальців, описані алгоритми, за якими оцінюються відбитки пальців, такі як NFIQ та виділення фону й оцінка яскравості, які в свою чергу доповнюють алгоритм NFIQ. Також був описаний алгоритм оцінки схожості, а саме MCC.

Результати, які будуть отримані за допомогою описаних алгоритмів, будуть у подальшому використані у підсистемі прийняття рішень на основі нечіткої логіки, яка буде побудована у наступному розділі.

4 ПОБУДОВА ПІДСИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Підсистема прийняття рішень приймає на вхід п'ять чисельних метрик для кожного з трьох відбитків: чотири метрики якості і одна метрика схожості з еталоном.

Як зазначалося вище, висновок на основі нечіткої логіки проводиться в три етапи і перший з них – фазифікації. Приведення чисельних метрик у значення лінгвістичних змінних проводиться за допомогою відповідних функцій приналежності.

4.1 Фазифікації схожості

При фазифікації, тобто отриманні лінгвістичних змінних метрики схожості, результатом є змінна *Identity* зі значеннями *Same* і *Different*. Обидва ці значення є нечіткими множинами. Їхні функції приналежності представлені на графіку (Рис. 4.1).

Метрика схожості, одержувана від алгоритму MCC, коливається від 0 до 1, де 1 означає абсолютно однаковий відбиток, а значення, близькі до 0, – різні. Ця метрика береться в якості аргументу функцій приналежності, і в результаті обчислення виходять ступені приналежності для відповідних змінних.

Наприклад, якщо відповідь за алгоритмом MCC дорівнює 0.6, то ступінь входження *Identity Same* буде 0.88, а *Identity Different* – 0.12.

Функція приналежності:

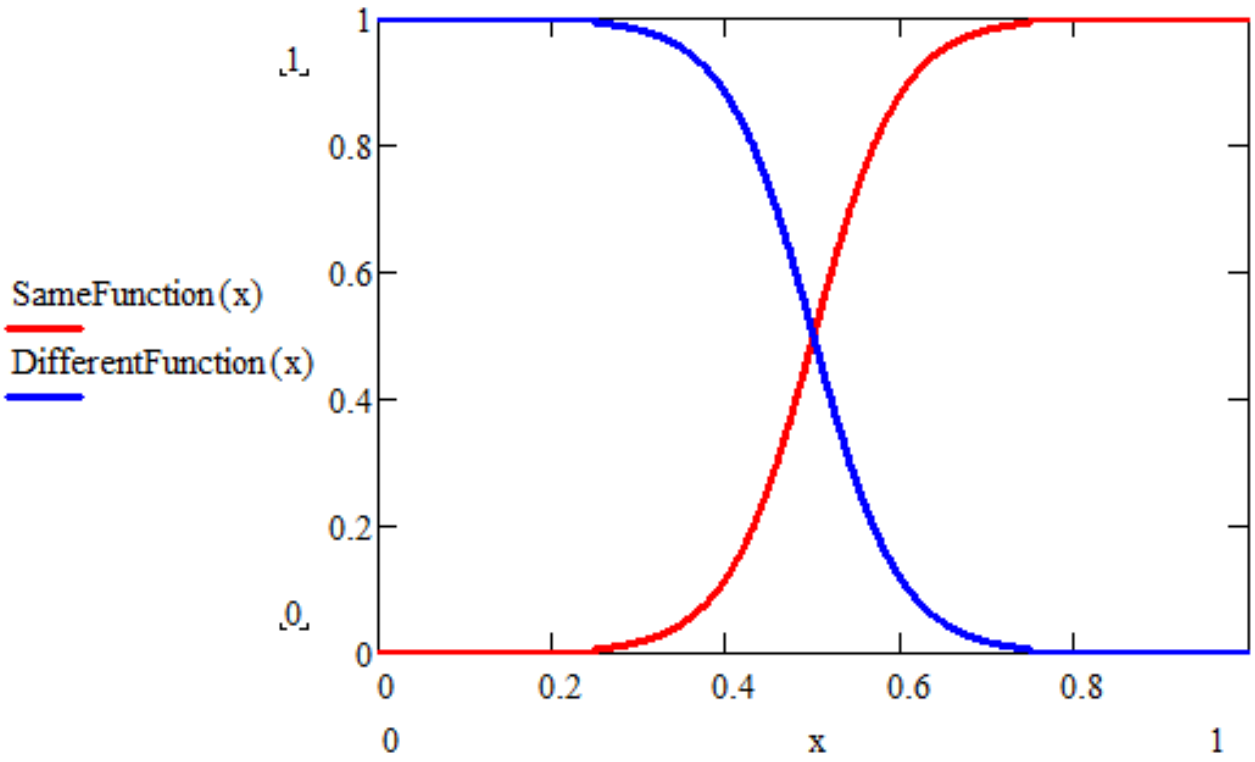

Рисунок 4.1 – Графік функції приналежності змінної *Identity*

Зсув даного графіка (Рис. 4.1) семантично відповідає зміні граничного значення порівняння в класичних системах розпізнавання.

4.2 Фазифікації якості

Аналогічно тому, як проводилася фазифікація якості, лінгвістичні змінні виводяться для метрик якості. Далі для кожної з них буде описана область допустимих значень, що отримується, змінна і функції приналежності її значень.

Метрика середньої якості

Метрика середньої якості алгоритму NFIQ змінюється в межах від 0 до 5, де 0 – низька якість, 5 – найвища.

Отримана змінна – *QualityNfiq* зі значеннями *Low* і *High*.

Функція приналежності:

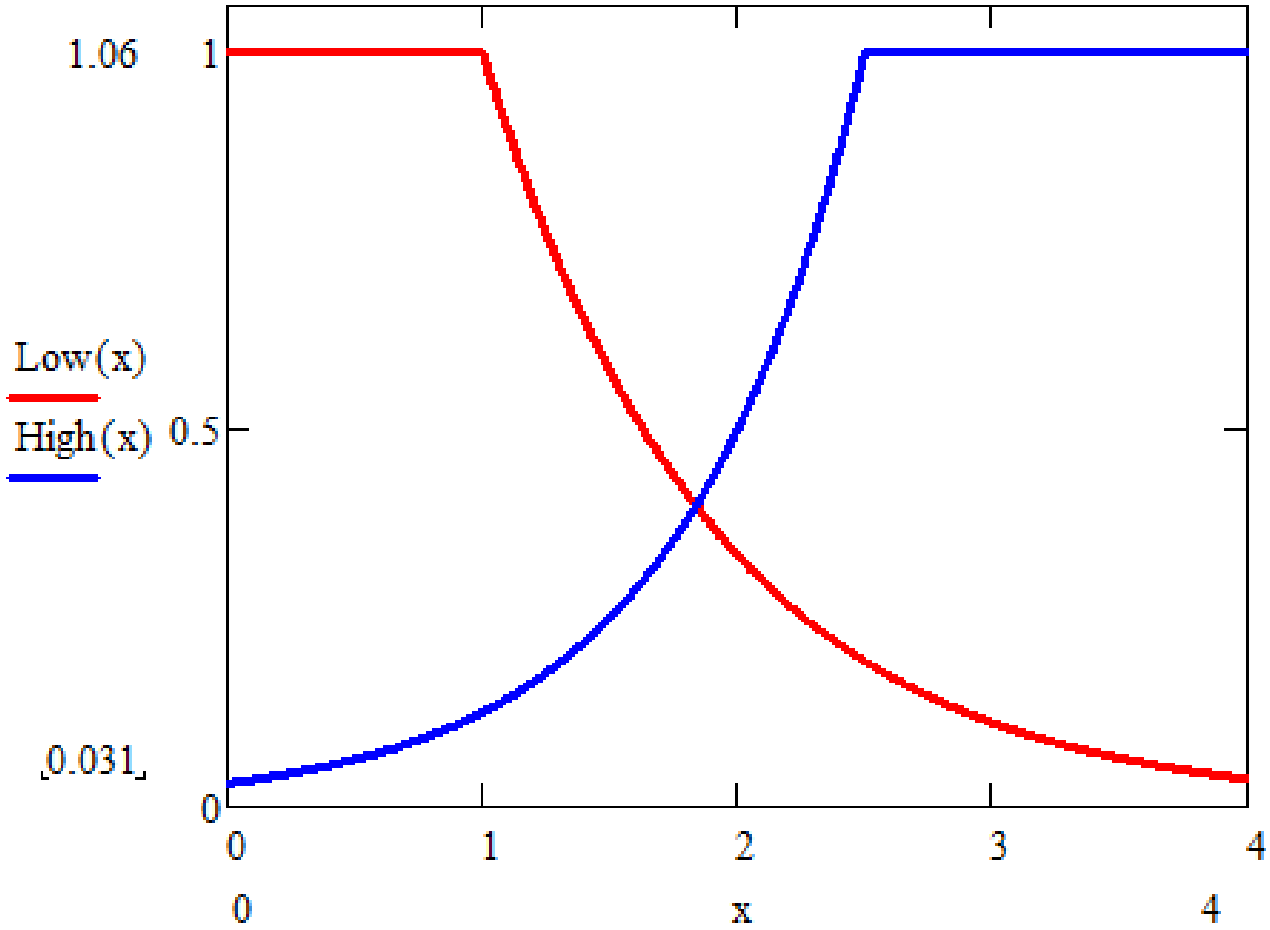

Рисунок 4.2 – Графік функції приналежності змінної *QualityNfiq*

Метрика відсотка блоків низької якості

Метрика кількості блоків низької якості за алгоритмом NFIQ коливається від 0 до 100. Блоками низької якості вважаються ті, у яких оцінка NFIQ 0 або 1.

Отримана змінна – *LowQualityBlocks* зі значеннями *Little* і *Many*.

Функція приналежності:

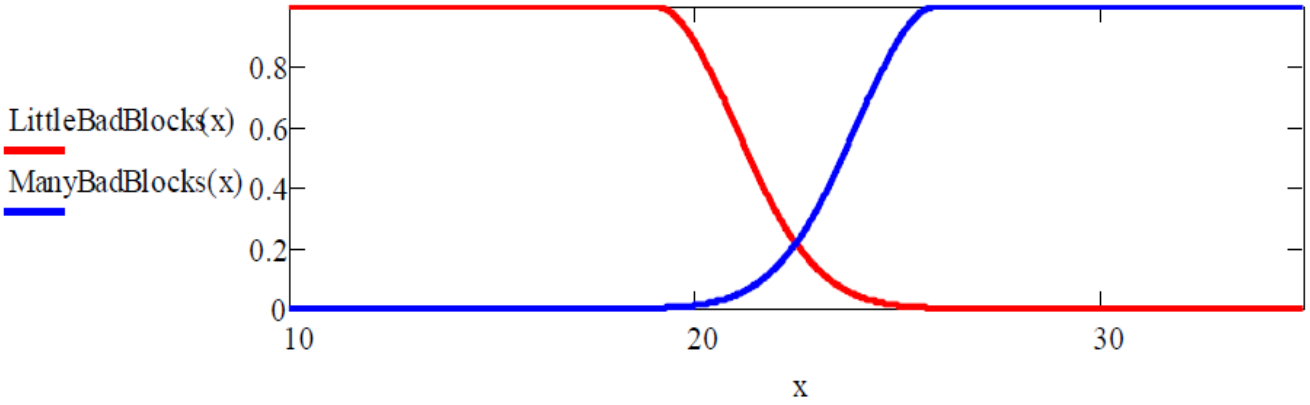

Рисунок 4.3 – Графік функції приналежності змінної *LowQualityBlocks*

Графік функцій побудований для значень від 10 до 40. Поза розглянутим діапазоном значення функцій не змінюються.

Метрика яскравості

Метрика яскравості відбитка також змінюється в межах від 0 до 100.

При цьому значення, близькі до 0, характеризують нормальний відбиток, а великі значення – темний.

Отримана змінна – *Brightness* зі значеннями *High* і *Low*.

Функція приналежності:

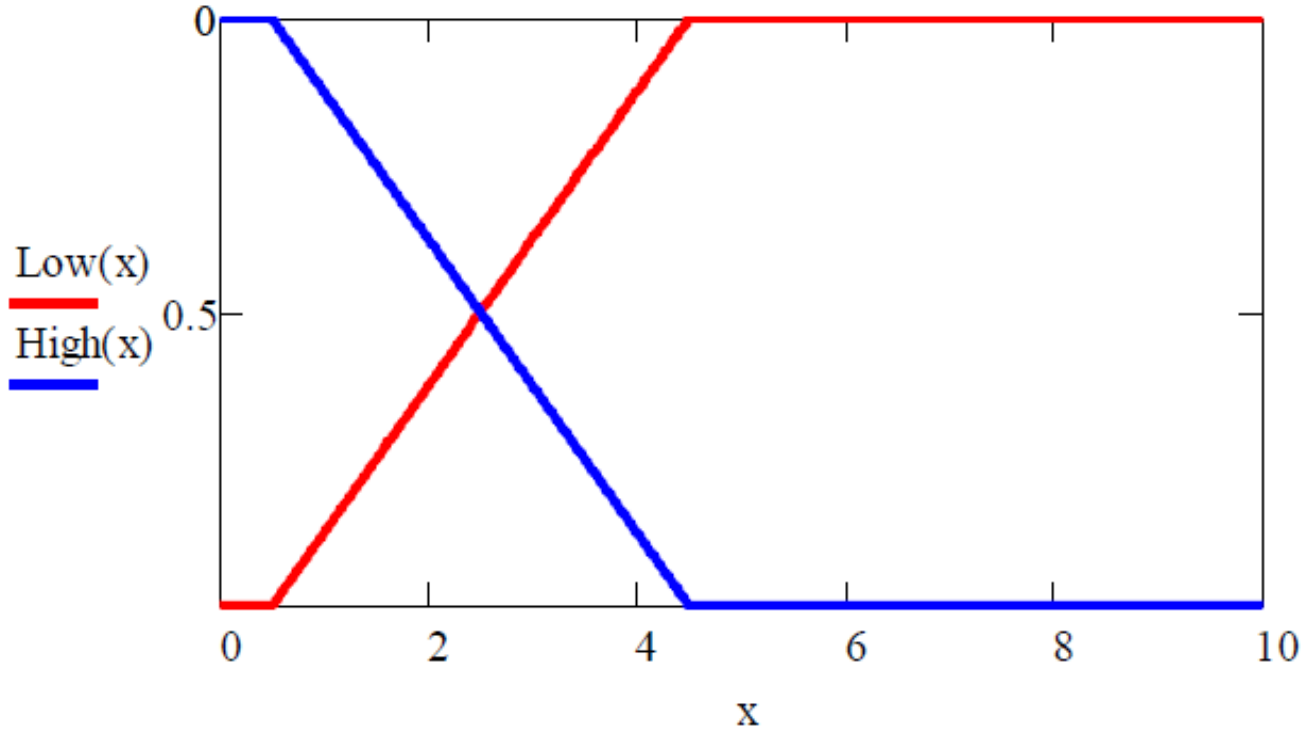

Рисунок 4.4 – Графік функції приналежності змінної *Brightness*

Графік функцій побудований для значень від 0 до 10. Поза розглянутим діапазоном значення функцій не змінюються.

Метрика відсотка фону

Метрика відсотка фону коливається між 0 і 100.

Отримана змінна – *Background* зі значеннями *Large* і *Normal*.

Функція приналежності:

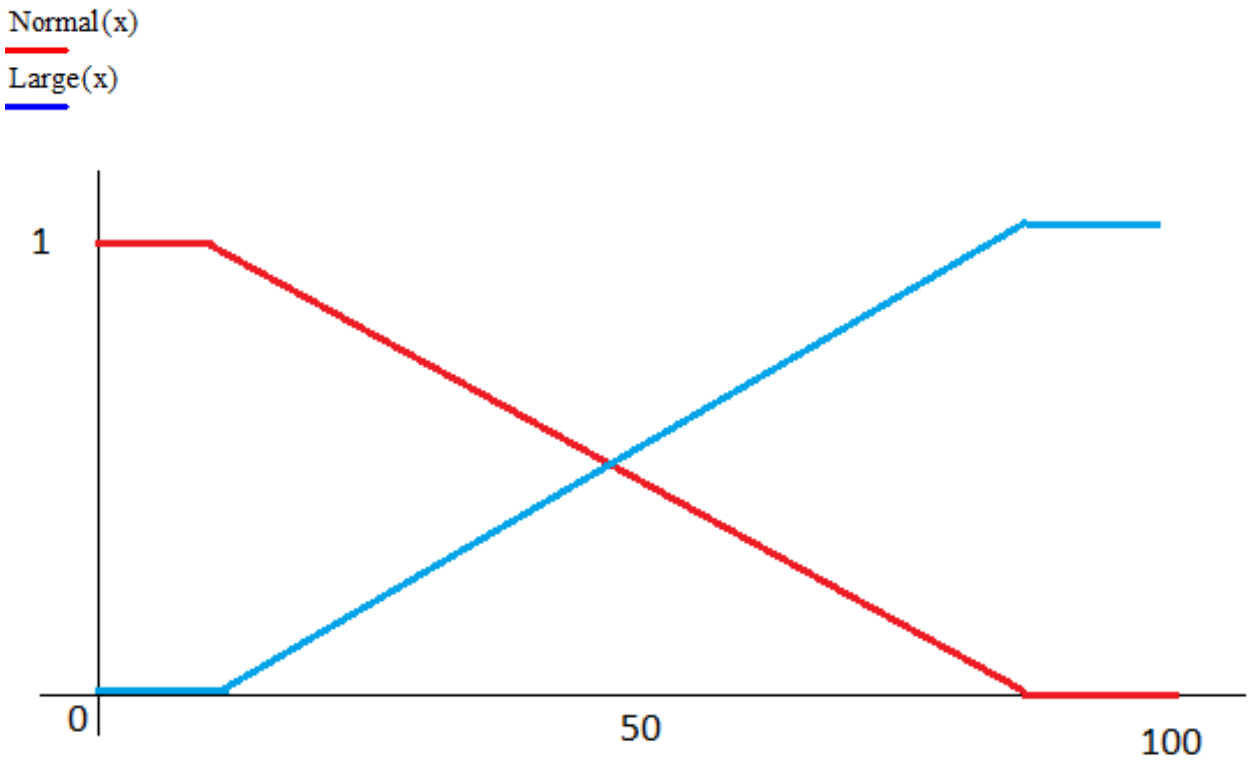

Рисунок 4.5 – Графік функції приналежності змінної *Background*

Вигляд даних функцій приналежності був визначений емпірично.

4.3 Метод навчання за допомогою нечіткої логіки

Наступний етап нечіткого виводу – застосування правил. Перед початком цього етапу правила зчитуються з файлу. На вхід подаються лінгвістичні змінні, отримані при фазифікації.

Так як одночасно існують всі значення лінгвістичної змінної, висновок йде за всіма правилами, де вона зустрічається в посилці. Для обчислення ступеня приналежності посилки використовуються максимінні операції. Далі, якщо значення змінної в кінцевому випадку ще не існує, воно створюється зі ступенем приналежності рівній ступеню приналежності посилки. Якщо ж воно існує, то ступінь приналежності визначається як максимум з існуючої та виведеної [5].

Вивід змінної якості

Спочатку виводиться змінна *Quality* зі значеннями *Low*, *Middle* і *High*. Вона показує загальне значення якості для відбитка. Так як правил досить багато, буде описаний принцип їх побудови.

Правила виведення змінної якості будувалися за таким принципом:

- якщо всі значення в посилці високі, то значення якості – високе;
- якщо одне із значень в посилці низьке, то якість – середня;
- якщо більше одного найнижчого значення, то якість – низька.

Приклад правила:

$Brightness\ high \wedge Background\ normal \wedge QualityNfiq\ high \wedge LowQualityBlocks\ little \Rightarrow Quality\ high$

$\wedge$ – в даному випадку означає логічне "І" або кон’юнкцію. Тобто в даному випадку це правило означає наступне: якщо у зображення висока яскравість, невелика кількість фону, якість за оцінкою алгоритму NFIQ висока і блоків низької якості мало, то його якість висока.

Вивід відповіді для одного відбитка

У цій частині виведення використовуються змінна якості та змінна схожості, й правила будуються за наступним принципом:

- якщо якість висока, то відповідь збігається зі змінною схожості;
- якщо якість середня, відповідь з коефіцієнтом $\frac{1}{2}$ збігається зі змінною схожості і з коефіцієнтом $\frac{1}{2}$ невідомий;
- якщо якість низька, відповідь невідома.

Приклад правила:

$Quality\ high \wedge Identity\ same \Rightarrow FingerPrintAnswer\ YES$

$Quality\ middle \wedge Identity\ different \Rightarrow FingerPrintAnswer\ NO$

$Quality\ low \wedge Identity\ same \Rightarrow FingerPrintAnswer\ IDK$

(IDK = I Don’t Know)

Вивід загальної відповіді для трьох відбитків

В останній частині правила застосовуються до відповідей від трьох відбитків пальців. Принцип побудови правил можна описати як узагальнення голосування простою більшістю на три відповіді. Тобто, якщо відповіді YES, NO та IDK уявити відповідно як 1, -1 та 0, то загальна відповідь буде виходити усередненням відповідей від трьох відбитків і округленням у бік збільшення модуля.

Приклад правила:

$F1\ YES \wedge F2\ YES \wedge F3\ IDK \Rightarrow Answer\ YES$

$F1\ YES \wedge F2\ YES \wedge F3\ NO \Rightarrow Answer\ YES$

$F1\ YES \wedge F2\ NO \wedge F3\ IDK \Rightarrow Answer\ IDK$

Отримавши загальну відповідь, ми дефазифікуємо його і в результаті отримуємо відповідь з найбільшим ступенем приналежності.

Висновки до розділу 4

У даному розділі була побудована підсистема прийняття рішень, в якій був застосований метод навчання за допомогою правил нечіткої логіки.

Проведена фазифікація дозволила визначити граничне значення побудованої системи, була взята точка перетину функцій належності значень *Identity Same* та *Identity Different*.

5 АНАЛІЗ І ПОРІВНЯННЯ

У зв'язку з імовірнісною природою усіх біометричних систем, прийняття рішення про ідентичність біометричних характеристих того чи іншого суб’єкта, не завжди дає позитивний результат для ідентичних відбитків, а для різних – негативний. Через це виникають помилки біометричних систем: відповідно, ймовірність помилкової відмови в доступі (False Rejection Rate, FRR), і ймовірність помилкового допуску (False Acceptance Rate, FAR). При порівнянні з граничним значенням, встановлення високого граничного значення призводить не тільки до зниження імовірності помилкового допуску, але і до зростання ймовірності помилкової відмови в допуску. Якщо ж виставлене низьке граничне значення, навпаки, зростає ймовірність помилкового допуску і зменшується помилкова відмова в допуску. Тому точність системи оцінюється коефіцієнтом рівної імовірності помилок (Equal Error Rate, EER) – це точка, де FAR = FRR (Рис. 5.1). В ідеальній ситуації графіки FAR та FRR не перетинаються, й значення ERR дорівнює нулю.

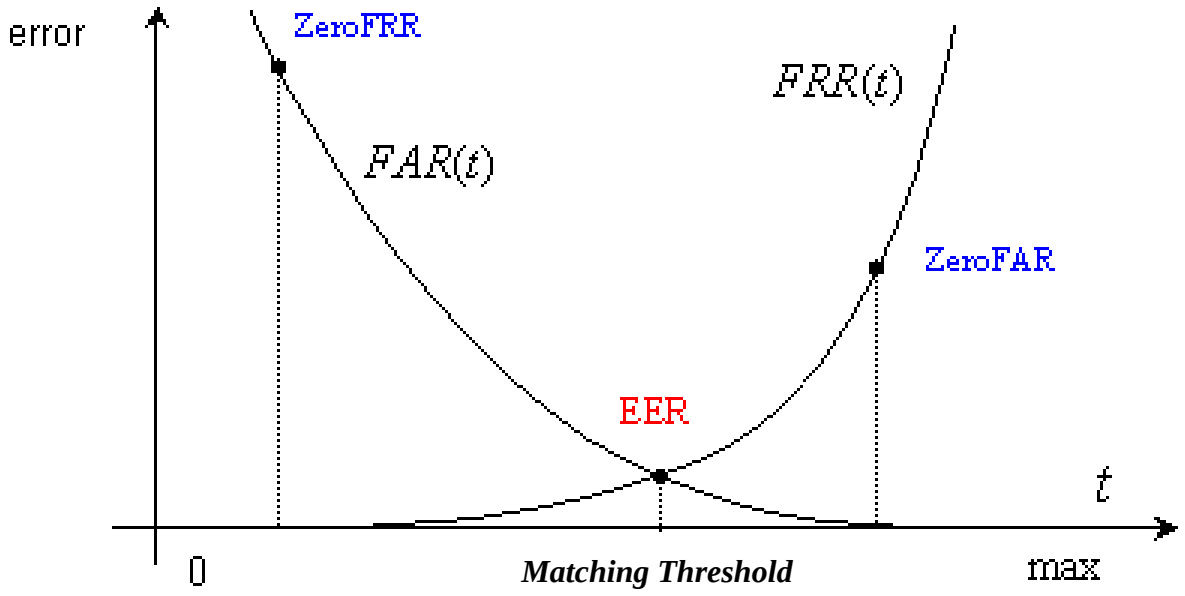

Рисунок 5.1 – Графік помилок FAR, FRR та EER

Для оцінки спроектованої системи були побудовані графіки коефіцієнтів рівної імовірності помилок (Equal Error Rate, EER) для визначення найкращого єдиного опису помилки. Чим нижче значення EER, тим менша імовірність появи помилок і тим більше адекватність алгоритму.

Для наборів даних DB1, DB2, DB3 і DB4, точки EER (0.2657, 0,00129), (0.2612, 0. 00214), (0.2005, 0.00103) і (0.2356, 0.0017) були записані, відповідно, як показано на рисунку 5.2.

Сенс даних результатів у тому, що для граничних значень 0,2657, 0,2612, 0.2005 і 0.2356 є гарантії одних і тих же коефіцієнтів помилок FAR і FRR 0.00129, 0.00214, 0.00103 і 0.0017 для алгоритму наборів даних DB1, DB2, DB3 і DB4 відповідно.

Це також означає, що 1,29, 2,14, 1,03 і 1,7 з кожних 1000 самозванців (або справжніх) спроби вдаються (або зазнають невдачі) на основі набору даних DB1, DB2, DB3 і DB4 відповідно.

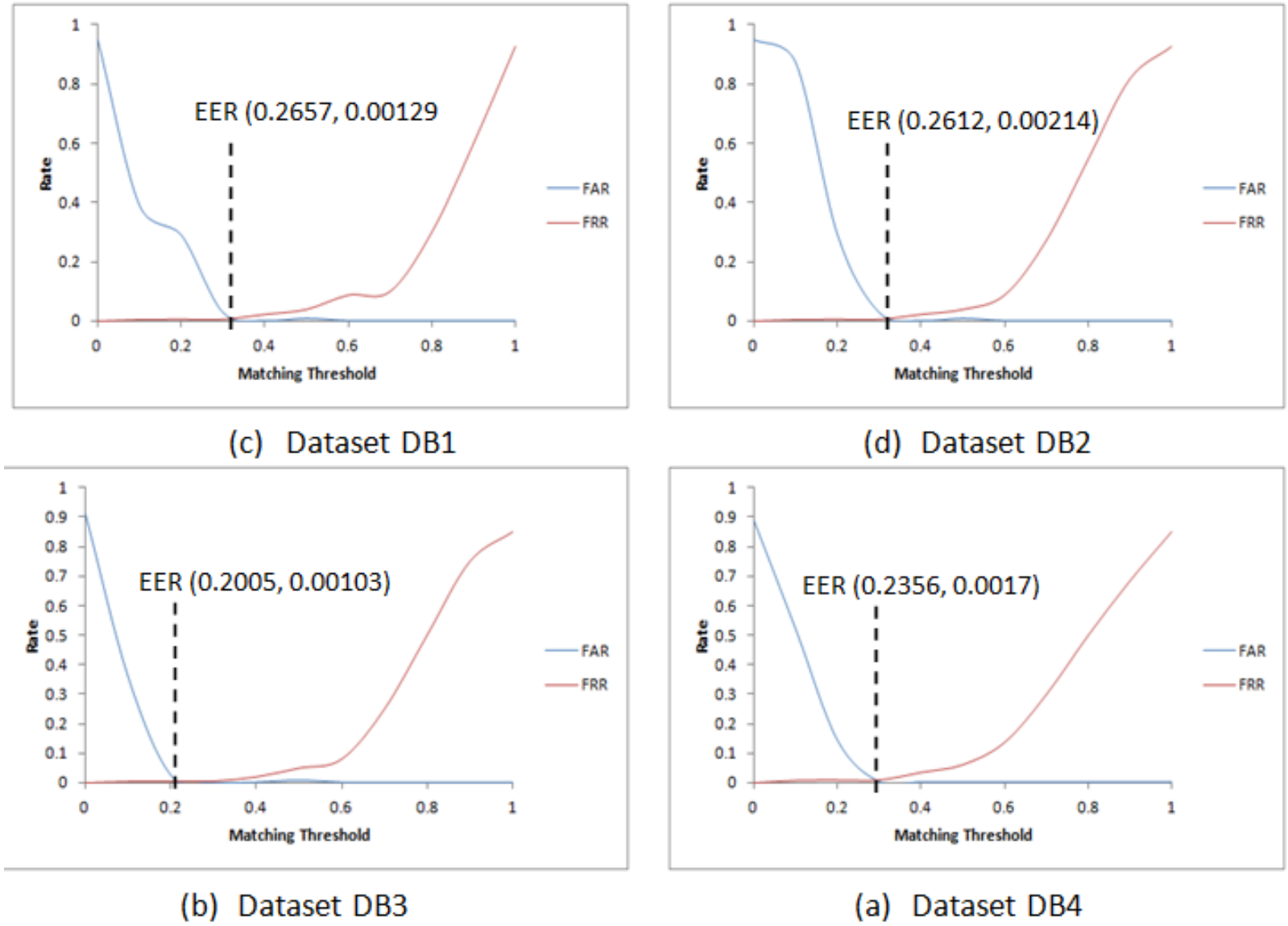

Рисунок 5.2 – Графік помилок FAR, FRR та EER

На рисунку 5.3 представлені отримані ROC-криві для чотирьох наборів даних. Криві виправдовують результати, отримані для FAR та FRR, зафіксувавши найвищу і найменшу FRR в нулі FAR для набору даних DB3 і DB1 відповідно.

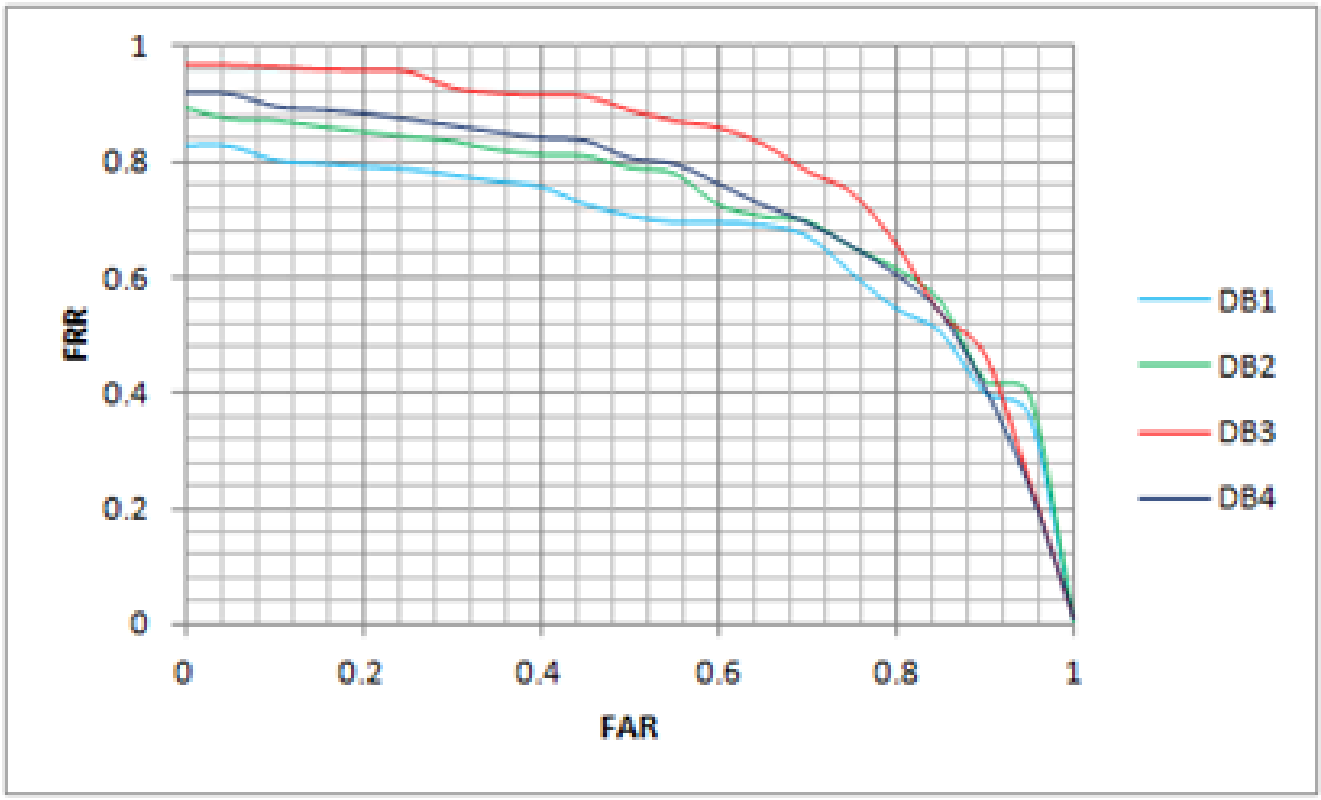

Рисунок 5.3 – ROC-криві для наборів даних DB1, DB2, DB3, DB4

5.1 Тестова множина відбитків пальців

Для тестування побудованої мультиекземплярної біометричної системи використовувалася відкрита база даних відбитків пальців FVC2000, DB2 набір A. Вона складається з 800 відбитків, по 8 відбитків на один палець. Кожен відбиток представлений у вигляді зображення в форматі .tif з розміром 364 x 256 пікселів і роздільною здатністю 500 dpi. Варто відзначити, що FVC2000 була побудована

саме для тестування систем розпізнавання відбитків пальців і містить багато відбитків низької якості. Для кожного пальця еталонним вважався відбиток кращої якості за NFIQ з даних восьми. При обчисленні імовірності помилкової відмови в доступі (FRR) з решти семи відбитків обиралися трійки відбитків. Вони і подавалися на вхід системі. Для обчислення імовірності помилкового доступу (FAR) трійки відбитків вибиралися випадково з усієї бази даних, за винятком відбитку цього пальця [15].

Значення якості відбитків і шаблони MCC кешуватися для зменшення часу роботи системи.

Результати розпізнавання системи з підсистемою прийняття рішення на основі нечіткої логіки порівнювалися з результатами розпізнавання схожих систем, кожна з яких відрізнялася від даної тільки блоком прийняття рішення. Це було зроблено для того, щоб виключити вплив інших факторів, не пов'язаних з системою прийняття рішення. Вони описані нижче:

1. Мономодальна система з порівнянням за граничним значенням.
2. Мультимодальна система з порівнянням за граничним значенням. Позитивна відповідь системи виноситься, якщо відповідь для кожного з трьох відбитків позитивна.
3. Мультимодальна система з порівнянням за граничним значенням. Відповідь системи визначається голосуванням простою більшістю.

Таблиця 5.1 – Порівняння ERR та граничних значень систем

	Система з нечіткою логікою	Мономодальна система	Мультимодальнана система з голосуванням	Мультимодальнана система з відповіддю три з трьох
ERR	**17.81%**	30.82%	29.3%	28.21%
Граничне значення	**0.525**	0.545	0.545	0.53

В якості граничного значення для мультиекземплярної біометричної системи з розпізнаванням на основі нечіткої логіки була взята точка перетину функцій належності значень *Identity Same* та *Identity Different.*

Висновки до розділу 5

У даному розділі був проведений аналіз і порівняння побудованої біометричної системи з розробленим методом прийняття рішень рішень на основі правил нечіткої логіки з іншими системами та стратегіями прийняття рішень.

Проведете тестування системи емпірично доводить те, що висновок рішення за допомогою нечіткої логіки дозволяє детально налаштувати процес прийняття рішення і дає можливість враховувати більшу кількість факторів.

ВИСНОВКИ

В ході виконання роботи були досягнуті наступні результати:

- вивчено предметну область систем розпізнавання відбитків пальців, а також основні принципи нечіткої логіки.
- розроблено новий метод прийняття рішень, який відрізняється використанням правил нечіткої логіки, що дозволяє підвищити ефективність мультимодальних біометричних систем.
- створено прототип мультиекземплярної системи для розпізнавання відбитків пальців, який використовує систему прийняття рішень на основі нечіткої логіки, алгоритм розпізнавання мінуцій MCC і алгоритм оцінки якості відбитків NFIQ.
- проведено порівняння результатів з альтернативними стратегіями прийняття рішень, що показав переваги алгоритму, заснованого на нечіткій логіці в порівнянні з іншими.

З усього вище зазначеного можна зробити висновок, що при збільшенні кількості модальностей виникає проблема прийняття рішення. У випадку з кількома модулями і, відповідно, декількома відповідями є наступні стратегії прийняття рішень:

- порівняння за граничним значенням і винесення позитивного рішення, якщо всі модулі відповіли позитивно. Цей випадок характеризується меншою ймовірністю помилкового допуску і більшою – помилкою відмови в допуску.
- порівняння за граничним значенням і голосування простою більшістю. Цей випадок, навпаки, підвищує ймовірність помилкового допуску і знижує – помилку відмови в допуску.
- висновок рішення за допомогою нечіткої логіки. Цей спосіб дозволяє детально налаштувати процес прийняття рішення і дає можливість враховувати більшу кількість факторів.

Тенденції розвитку біометрії й засновані на її принципах системи стали ефективним засобом убезпечення всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі та поліпшення іхньої ефективності є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектора, індустріальних і комерційних структур, так і для окремих громадян.