

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ
БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ
ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

*Кваліфікаційна робота містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

(підпис) Богдан ОСАДЧИЙ
Ім'я, ПРИЗВИЩЕ здобувача

Виконав:	Здобувач вищої освіти гр. УБДМ 61 Богдан ОСАДЧИЙ
Керівник:	Тетяна МУЖАНОВА
к.держ.упр., доц	
Рецензент:	_____

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедри УІКБ

_____ Світлана ЛЕГОМІНОВА

“ _____ ” _____ 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

студенту Осадчому Богдану Ігоровичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доц.

(Ім'я, ПРИЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19” жовтня 2023 р. № 145.

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: управління інформаційною безпекою, біометричні технології ідентифікації, технології мультимодальної біометричної верифікації.
4. Перелік питань, які потрібно розробити:
 1. Дослідити історію виникнення й основні види біометричних технологій.
 2. Встановити особливості й переваги систем мультимодальної біометричної ідентифікації.
 3. З'ясувати роль біометричних технологій в управлінні доступом.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Дослідження історії виникнення й основних видів біометричних технологій.	27.10.2023	
4.	Дослідження особливостей й переваг систем мультимодальної біометричної ідентифікації.	10.11.2023	
5.	Визначення ролі біометричних технологій в управлінні доступом.	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	.01.2024	

Здобувач вищої освіти

(підпис)

Богдан ОСАДЧИЙ

(Ім'я, ПРІЗВИЩЕ)

Керівник
кваліфікаційної роботи

(підпис)

Тетяна МУЖАНОВА

(Ім'я, ПРІЗВИЩЕ)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра**

Направляється здобувач Осадчий Б. І. до захисту кваліфікаційної роботи
(*прізвище та ініціали*)

за спеціальністю 125 Кібербезпека
(*код, найменування спеціальності*)

Освітньо-професійної програми Управління інформаційною безпекою
(*назва*)

на тему: “ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ
ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ
БЕЗПЕКОЮ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____
(*підпис*)

Віталій САВЧЕНКО
(*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач **ОСАДЧИЙ Богдан** у кваліфікаційній роботі дослідив історію виникнення й основні види біометричних технологій; встановив особливості й переваги систем мультимодальної біометричної ідентифікації, з'ясував роль біометричних технологій в управлінні доступом.

ОСАДЧИЙ Богдан оформив кваліфікаційну роботу відповідно до вимог. Виклад матеріалу здійснено згідно з планом, зроблено відповідні висновки. Ключові положення роботи представлено у вигляді зображень. Здобувач показав хороші теоретичні та практичні знання, вміння проводити дослідження і самостійно вирішувати наукові завдання.

Результати дослідження апробовані на конференції “Актуальні проблеми кібербезпеки” 2023 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ОСАДЧОГО Богдана** на позитивну оцінку та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційної роботи _____
(*підпис*)

Тетяна МУЖАНОВА
(*Ім'я, ПРІЗВИЩЕ*)

“ ____ ” _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Осадчий Б. І. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою

(*підпис*)

Світлана ЛЕГОМІНОВА
(*Ім'я, ПРІЗВИЩЕ*)

ВІДГУК РЕЦЕНЗЕНТА **на кваліфікаційну магістерську роботу**

Здобувача вищої освіти Осадчого Богдана Ігоровича

На тему: ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ
ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ
БЕЗПЕКОЮ

Актуальність: У сучасних умовах постійного розвитку цифрових технологій і зростання кількості кіберзагроз нагальною є необхідність забезпечення високого рівня інформаційної безпеки. Одним із ключових напрямів забезпечення безпеки є управління доступом та ідентифікація, які поряд із традиційними методами, такими як паролі чи картки доступу, все ширше використовують біометричні технології.

Біометричні технології, які базуються на перевірці унікальних фізичних чи поведінкових характеристик людини, забезпечують високу точність, надійність і невеликий відсоток помилкових спрацювань, що дозволяє значно підвищити рівень безпеки та запобігти несанкціонованому доступу.

У зв'язку з цим дослідження переваг і недоліків використання біометричних технологій ідентифікації в управлінні інформаційною безпекою є актуальним науковим завданням.

Позитивні сторони. У кваліфікаційній роботі досліджено історію виникнення й основні види біометричних технологій; встановлено особливості й переваги систем мультимодальної біометричної ідентифікації; з'ясовано роль біометричних технологій в управлінні доступом.

Здобувач оволодів методами наукового дослідження, опрацював достатню джерельну базу за предметом дослідження. Кваліфікаційна робота оформлена у відповідності з вимогами, а її структура забезпечує досягнення мети і завдань.

Недоліки

1. Доцільно було б навести більше прикладів практичного використання систем мультимодальної біометричної ідентифікації, в т.ч. з урахуванням вітчизняної специфіки.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на достатньому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувач Осадчий Богдан Ігорович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент:

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 91 стор., 13 рис., 1 табл., 124 джерела.

Метою роботи є дослідження переваг і недоліків використання біометричних технологій ідентифікації в управлінні інформаційною безпекою.

Об'єктом дослідження є технології ідентифікації в управлінні інформаційною безпекою.

Предмет дослідження – переваги й недоліки використання біометричних технологій ідентифікації в управлінні інформаційною безпекою.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи системного аналізу, синтезу, порівняння та теоретичного узагальнення, класифікації, математичні методи.

Короткий зміст роботи. Як результат у роботі досліджено історію виникнення й основні види біометричних технологій; встановлено особливості й переваги систем мультимодальної біометричної верифікації; роль з'ясовано біометричних технологій в управлінні доступом.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління доступом, заходів контролю робочого часу й автентифікації персоналу у контексті забезпечення інформаційної безпеки підприємства.

КЛЮЧОВІ СЛОВА : УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ, ТЕХНОЛОГІЇ МУЛЬТИМОДАЛЬНОЇ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 91 pages, 13 figures, 1 table, 124 sources.

The purpose of the study is to investigate the advantages and disadvantages of using biometric identification technologies in information security management.

Object of research is identification technologies in information security management.

Subject of research is the advantages and disadvantages of using biometric identification technologies in information security management.

Research methods. To solve the above-mentioned scientific task, the methods of system analysis, synthesis, comparison and theoretical generalization, classification, mathematical methods were used in the work.

Brief content of research. As a result, the paper investigates the history of the emergence and main types of biometric technologies; the features and advantages of multimodal biometric verification systems; the role of biometric technologies in access control.

Field of research. The developed approaches can be used in the planning and implementation of access control systems, time tracking and authentication of enterprise employees in the context of counteracting threats related to biometric identification.

KEYWORDS: INFORMATION SECURITY MANAGEMENT, BIOMETRIC IDENTIFICATION TECHNOLOGIES, MULTIMODAL BIOMETRIC VERIFICATION TECHNOLOGIES.

ЗМІСТ

ВСТУП.....	10
РОЗДІЛ 1 ІСТОРІЯ ВИНИКНЕННЯ Й ОСНОВНІ ВИДИ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ	12
1.1 Розвиток і застосування сучасних біометричних технологій	12
1.2 Види біологічної біометрії	20
1.2.1 Візуальна біометрія.....	21
1.2.2 Хімічна біометрія	26
1.2.3. Просторова біометрія	27
1.3 Об'єкти й технології поведінкової біометрії.....	31
Висновки до розділу 1	36
РОЗДІЛ 2 ОСОБЛИВОСТІ Й ПЕРЕВАГИ СИСТЕМ МУЛЬТИМОДАЛЬНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ.....	37
2.1 Загрози і вразливості біометричних систем та їх захист	37
2.1.1 Типи ворожих атак	37
2.1.2 Захист апаратного забезпечення	38
2.1.3 Надійне зіставлення відбитків пальців	39
2.2 Мультимодальні біометричні системи	44
2.2.1 Бази даних і протоколи.....	46
2.2.2 Опис базової системи	48
2.2.3 Базові системні класифікатори.....	50
2.3 Приклади мультимодальних систем розпізнавання особи	51
Висновки до розділу 2	57
РОЗДІЛ 3 БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ ДОСТУПОМ	58
3.1 Складові біометричних систем контролю і управління доступом	58
3.1.1 Біометричні зчитувачі	59
3.1.2 Біометричні контролери	61
3.1.3 Біометричні термінали	61
3.2 Огляд технічних засобів біометричних СКУД бренду ZkTeco	63
3.2.1 Біометричні зчитувачі ZkTeco FR1500	63
3.2.2 Біометричні контролери ZkTeco inBio160/260/460	64

3.2.3 Біометричні термінали ZKTeco WL30.....	66
3.2.4 Мультибіометричні термінали ZKTeco FV18.....	67
3.2.5 Мультибіометричні термінали ZKTeco Multibio700.....	68
3.3 Технологія розпізнавання обличчя Face ID.....	70
3.3.1 Сфери застосування Face ID.....	71
3.3.2 Розпізнавання живої присутності.....	75
Висновки до розділу 3	78
ВИСНОВКИ.....	79
СПИСОК ПОСИЛАНЬ	81

ВСТУП

Актуальність теми. У сучасному світі нагальною є необхідність забезпечення високого рівня інформаційної безпеки в умовах постійного розвитку цифрових технологій і зростання кількості кіберзагроз. Одним із ключових напрямів забезпечення безпеки є управління доступом та ідентифікація, які поряд із традиційними методами, такими як паролі чи картки доступу, все ширше використовують біометричні технології.

Біометричні методи, які базуються на перевірці унікальних фізичних чи поведінкових характеристик людини, забезпечують високу точність, надійність і невеликий відсоток помилкових спрацювань, що дозволяє значно підвищити рівень захисту конфіденційної інформації та запобігти несанкціонованому доступу до неї. Однак, біометричним системам притаманні потенційні недоліки і вразливості, які також потребують ретельного вивчення.

Актуальність дослідження цієї теми полягає в необхідності забезпечення збалансованого підходу до використання біометричних технологій з метою підвищення ефективності забезпечення інформаційної безпеки підприємства.

Мета роботи полягає у дослідженні переваг і недоліків використання біометричних технологій ідентифікації в управлінні інформаційною безпекою.

Об'єкт дослідження - технології ідентифікації в управлінні інформаційною безпекою.

Предмет дослідження – переваги й недоліки використання біометричних технологій ідентифікації в управлінні інформаційною безпекою.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання*:

1. Дослідити історію виникнення й основні види біометричних технологій.
2. Встановити особливості й переваги систем мультимодальної біометричної верифікації.
3. З'ясувати роль біометричних технологій в управлінні доступом.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи системного аналізу, синтезу, порівняння та теоретичного узагальнення, класифікації, математичні методи.

Наукова новизна одержаних результатів. У роботі досліджено особливості й переваги систем мультимодальної біометричної ідентифікації, з'ясовано роль біометричних технологій в управлінні доступом, а також проаналізовано функціонал біометричних елементів СКУД від виробника ZKTeco.

Практичне значення одержаних результатів. Застосування напрацювань надасть можливість здійснити обґрунтований вибір методів і засобів біометричної ідентифікації у рамках системи управління інформаційною безпекою підприємства.

Апробація результатів кваліфікаційної роботи була здійснена на конференції “Актуальні проблеми кібербезпеки” 2023 року.

РОЗДІЛ 1

ІСТОРІЯ ВИНИКНЕННЯ Й ОСНОВНІ ВИДИ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

1.1 Розвиток і застосування сучасних біометричних технологій

У сучасному світі біометрія визначається як синтез технологічних та наукових методів автентифікації, заснованих на біологічних особливостях людини, що широко застосовуються в інформаційному забезпеченні [1]. Це вимірювання та статистичний аналіз, спрямовані на виявлення унікальних інтелектуальних і поведінкових особливостей. Головним призначенням біометрії є ідентифікація та контроль доступу, а також встановлення осіб, за якими ведеться спостереження. Основний принцип біометричної верифікації полягає в можливості точного визначення особи на підставі її внутрішніх фізичних або поведінкових характеристик.

Термін "біометрія" має грецьке походження, де "метрика" означає вимірювання, а "біо" – життя. Отже, біометрія визначає ідентифікацію за допомогою частин тіла. Застосовуючи біометрію, можна забезпечити автентичність ідентифікації, використовуючи біологічну інформацію людини [2], таку як сітківка ока [3], ДНК, відбитки пальців, голос і інші. Ці дані є загальними біометричними характеристиками, що робить біометрію унікальним і найнадійнішим методом для безпечної автентифікації будь-якої особи.

Біометричні технології стали важливою складовою сучасного інформаційного суспільства, впроваджуючи нові стандарти безпеки та автентифікації. Використовуючи унікальні фізичні і поведінкові характеристики особи, біометрія забезпечує надзвичайно надійні методи ідентифікації, що перевершують традиційні методи, такі як паролі чи картки доступу.

Однією з ключових переваг біометричних технологій є їхній високий рівень надійності та важливість у вирішенні проблем безпеки. Такий метод автентифікації базується на тому, що кожна особа має унікальні фізичні або поведінкові риси, які практично неможливо підробити або скопіювати. Це робить біометрію ідеальним рішенням для захисту конфіденційної інформації, фінансових транзакцій та особистих даних.

Однією із найпоширеніших форм біометричної ідентифікації є використання відбитків пальців. Інші види біометричних даних включають сітківку ока, голосовий зразок, геометрію обличчя та навіть генетичний код. Ці дані використовуються для створення унікального "біометричного шаблону" кожної особи, який служить основою для подальшої ідентифікації.

Застосування біометричних технологій розповсюджується в різних галузях, включаючи фінанси, медицину, сферу громадської безпеки та інформаційні технології. Невпинний розвиток цих технологій відкриває нові можливості для покращення безпеки та зручності у різних аспектах нашого повсякденного життя. Однак, разом із зростанням їхнього використання, виникають також питання щодо приватності та етики, які потребують уважного вирішення.

На рисунку 1.1 зображено різні типи біометрії [4].

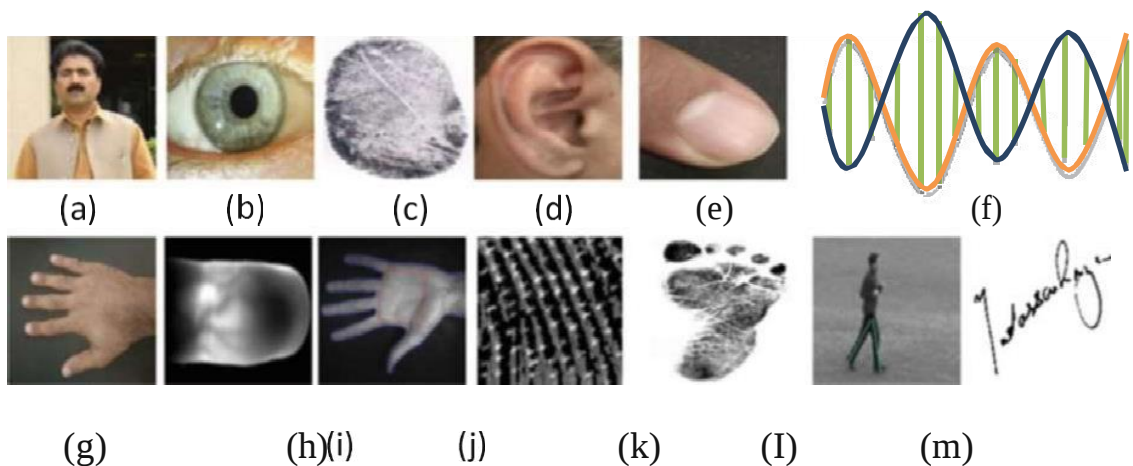


Рис. 1.1. Біометричні типи (a) обличчя, (b) райдужна оболонка ока, (c) відбиток пальця, (d) вухо, (e) кусочок нігтя, (f) ДНК, (g) рука, (h) вена пальця, (i) вена долоні, (j) потові пори, (k) відбиток стопи, (l) хода, (m) підпис

Системи управління біометричною ідентифікацією (BIMS) встановлюють найвищі стандарти безпеки, враховуючи такі ключові аспекти, як довіра, зручність, відповідальність та систематичний аудит. Ці важливі функції служать основою для пошуку та впровадження компаніями передових технологій з метою досягнення своїх стратегічних цілей.

У сучасному світі біометричні технології знаходять широке застосування у різних сферах, включаючи, але не обмежуючись:

- Банківська автентифікація.
- Безпека в аеропортах.
- Національний рівень ідентифікації.
- Діяльність правоохоронних органів.
- Контроль доступу та єдиний вхід (SSO).
- Ведення обліку робочого часу та відвідувань.

Безумовно, створення надійної біологічної системи є викликом, і термін "біометрична технологія" визначається як ідеальна альтернатива у галузі безпеки. Результати численних досліджень спрямовані на вдосконалення процесів розпізнавання осіб за допомогою біометричних даних, і, незважаючи на досягнені успіхи, залишається простір для подальших інновацій та вдосконалень. Біометричні технології продовжують еволюцію, а їхнє застосування в різних галузях не тільки підвищує рівень безпеки, а й сприяє зручності та ефективності у вирішенні різноманітних завдань.

Тривала еволюція біометричних технологій сприяє їхньому поширенню в нових сферах, розширюючи можливості застосування та підвищуючи рівень безпеки в різних аспектах життя. Зокрема, біометрія стає невід'ємною частиною фінансового сектору, забезпечуючи високий рівень автентифікації в банківських операціях та зменшуючи ризик фінансових шахрайств.

У сфері безпеки аеропортів біометричні технології використовуються для швидкої та надійної ідентифікації пасажирів, що сприяє покращенню процесу перевірки та прискорює пасажирські потоки.

Національні системи ідентифікації, які базуються на біометричних технологіях, забезпечують надійний ідентифікаційний фундамент, важливий для вирішення численних соціальних та економічних завдань, включаючи видачу паспортів та інших документів.

Правоохоронні органи використовують біометричні технології для швидкого виявлення та ідентифікації злочинців, що сприяє забезпеченню громадської безпеки та викриттю злочинів.

Контроль доступу та єдиний вхід (SSO) на основі біометричних даних дозволяють компаніям ефективно захищати конфіденційну інформацію та обмежувати доступ лише авторизованим особам.

У сфері обліку робочого часу та відвідувань біометричні системи забезпечують точність та достовірність даних, що допомагає підвищити ефективність управління персоналом та вдосконалити робочі процеси.

І незважаючи на досягнені успіхи в області біометричних технологій, постійний науковий та технологічний прогрес відкриває нові можливості для подальших вдосконалень та розширення їхнього застосування в різних сферах суспільства, використовуючи прогрес технологій минулого.

Біометричні технології базуються на використанні фізіологічних або поведінкових характеристик людини для ідентифікації або верифікації її особи. Ці технології виникли як відповідь на потребу у вдосконаленні систем ідентифікації та забезпеченні безпеки в різних областях.

Історичні етапи виникнення і розвитку біометричних технологій

Перші спроби використання фізіологічних рис людини для ідентифікації можна віднести до палеографії та дактилоскопії. У середньовіччі сформувалися перші погляди на унікальність папілярних ліній пальців.

Палеографія - це наука, що вивчає історію письма, його розвиток та особливості на різних етапах еволюції. Основним об'єктом дослідження є графічні форми знаків та літер, їхні пропорції, конфігурації, а також шрифти. Особливу увагу приділяється місцю і частоті вживання окремих літер, а

також різноманітним стилістичним особливостям письма, таким як види скорочень та інші характеристики [5].

Дактилоскопія є розділом криміналістики, що вивчає конфігурацію папілярних ліній на пучках пальців рук для встановлення особистої ідентифікації. Цей метод ідентифікації, заснований на унікальності малюнка шкіри, був винайдений Вільямом Джеймсом Гершелем у 1877 році. Гершель, який служив поліцейським у Індії, запропонував гіпотезу про постійність папілярного малюнка на поверхні долонь людини [6].

Ідея унікальності відбитків пальців вже існувала в Китаї та Японії у VII столітті н.е. Незважаючи на широке використання цього методу, припущення про унікальність відбитків не має належного наукового обґрунтування, і немає достатніх доказів щодо повної достовірності цього методу ідентифікації (хоча на практиці його часто вважають абсолютно надійним). З розвитком технологій у XX ст., зокрема поява фотографії і розвиток комп'ютерів, стали можливими більш складні методи ідентифікації. Виникли перші системи розпізнавання обличчя, голосу й інших біометричних параметрів.

Перші дослідження в галузі розпізнавання обличчя відбувалися протягом 1960-1970 років та здійснювались в основному в рамках академічних досліджень та військових дослідницьких проектів. Техніка була обмеженою і в основному базувалася на ручних методах аналізу фізіономії. У 1980-1990 роках з появою комп'ютерів та покращенням алгоритмів обробки зображень розпочалося використання автоматизованих систем розпізнавання обличчя. Одні з перших систем стали використовувати геометричні особливості обличчя для ідентифікації. Після 2000 року з появою більш потужних обчислювальних систем та розвитком технологій машинного навчання та глибокого навчання відбулася значна еволюція систем розпізнавання обличчя. Сучасні системи можуть працювати в реальному часі та враховувати різноманітні умови освітлення та вигляду обличчя.

Перші дослідження в області розпізнавання голосу розпочалися в середині 20-го століття, коли були розроблені перші механічні системи для

розпізнавання фонетичних особливостей. З розвитком електроніки та комп'ютерів у 1960-1990 роках почали виникати перші експериментальні системи розпізнавання голосу. Вони використовували базові акустичні та фонетичні моделі. У 1980-1990 роках розпочалась активна розробка систем розпізнавання голосу на основі технік мовленнєвого аналізу та використання статистичних методів. Після 2000 року використання методів машинного навчання та глибокого навчання дозволило покращити точність систем розпізнавання голосу. Сучасні голосові асистенти та системи розпізнавання мови стали широко поширеними в різних сферах [6].

З поширенням комп'ютерів та Інтернету зросла потреба у вдосконаленні систем безпеки. Біометричні технології знайшли широке застосування в сферах фінансів, охорони праці, контролю доступу та інших.

Завдяки розвитку стандартів і промислових нормативів, біометричні технології отримали більшу визначеність і стали більш придатними для широкого застосування. Проте стандартизація може бути як локальна (в межах певної сфери або країни), так і міжнародна.

До міжнародних організацій належать організації, такі як Міжнародна організація зі стандартизації (ISO) та Міжнародний комітет з електротехніки (IEC), які розробляють стандарти для біометричних технологій. Ці стандарти визначають методи та протоколи для забезпечення сумісності та взаємодії між різними біометричними системами. Деякі види робіт виконуються спільними зусиллями ISO та IEC. Наприклад, питання інформаційних технологій, мікропроцесорної техніки тощо - це об'єкти спільних розробок ISO/IEC.

На сьогодні фахівцями цих організацій розроблена серія стандартів ISO/IEC 27000, яка постійно доповнюється новими документами. В Україні прийнято стандарт серії ДСТУ ISO/IEC 27001:2023 [7], який зібрав описи найкращих світових практик в області управління інформаційною безпекою. Документ встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження,

функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки.

Також в Україні прийнято новіший стандарт ДСТУ ISO/IEC 27009:2018 [8]. Метою розробки документу є забезпечення захисту інформації конкретних секторів: фінансів, транспорту та охорони здоров'я, а також інфраструктурних проектів, таких як смарт-міста. Серед інших, серія охоплює такі стандарти:

- ДСТУ ISO/IEC 27017:2017 [9] містить зведення правил щодо контролю за інформаційною безпекою для хмарних обчислювань.
- ДСТУ ISO/IEC 27013:2017 [10] пропонує комплексне рішення для послуг захисту інформації.

Також в Україні нещодавно прийнятий ДСТУ ISO/IEC 24745:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації (ISO/IEC 24745:2022, IDT) [11], який регламентує питання захисту біометричної інформації відповідно до вимог конфіденційності, цілісності й можливості поновлення/скасування під час зберігання та передачі.

Стандарт встановлює вимоги і рекомендації щодо безпечного й сумісного з конфіденційністю управління й обробки біометричної інформації і визначає:

- засади аналізу загроз і заходів їх протидії, властивих біометрії та моделям застосування біометричних систем;
- вимоги безпеки для безпечного зв'язку між біометричним посиленням (BR) та посиленням на ідентифікацію (IR);
- прикладні моделі біометричних систем із різними сценаріями зберігання та порівняння БР;
- вказівки щодо захисту приватного життя особи під час обробки біометричної інформації.

Багато країн розробляють власні нормативи та законодавство, що регулюють використання біометричних технологій. Це може включати в себе

питання захисту приватності, управління даними, правила доступу та інші аспекти використання біометричних ідентифікаторів.

Стандарти та нормативи щодо безпеки даних можуть значно відрізнятися в різних країнах через культурні, правові та економічні відмінності. Ось кілька прикладів незвичайних або особливих підходів до нормативного регулювання в галузі безпеки даних:

- Європейський Загальний регламент з захисту даних (GDPR) [12] стосується всіх країн Європейського Союзу та визначає вимоги до збору, обробки та збереження особистих даних. GDPR встановлює строгі норми щодо згоди, прав осіб на доступ до їхніх даних, а також вимагає відповідності від підприємств, які опрацьовують такі дані.

- Індія розглядає прийняття нового законодавства щодо збору та використання даних. Законопроект передбачає введення обмежень на збір та використання особистих даних, а також визначає обов'язки для підприємств у сфері обробки даних.

- Закон КНР про кібербезпеку [13] встановлює жорсткі вимоги щодо збереження даних в межах країни. Зокрема, важливі дані, зібрані в Китаї, повинні зберігатися на території країни, і для їх передачі за кордон потрібно одержувати спеціальні дозволи.

Ці приклади підкреслюють різноманітність підходів країн до регулювання безпеки даних та захисту приватності. У кожному випадку, нормативи відображають специфічні вимоги та цінності кожної країни в контексті її юридичної, соціокультурної та економічної ситуації.

Стандартизація також спрямована на вирішення питань захисту приватності та етичних аспектів використання біометричних даних. Наприклад, стандарти можуть встановлювати вимоги до збереження і обробки біометричних інформацій, а також забезпечувати прозорість і контроль для осіб, чий дані використовуються. Стандартизація і регулювання грають важливу роль у створенні довіри до біометричних технологій, а також в уніфікації та інтеграції різних систем. Це сприяє розвитку ринку та

забезпеченню високого рівня якості та безпеки при використанні біометричних ідентифікаторів.

З розвитком апаратних засобів, таких як високоякісні камери, сенсори відбитків пальців та інші, а також зростання потужності обчислювальної техніки, біометричні системи стали точнішими і швидшими.

1.2 Види біологічної біометрії

Автоматичне визначення особи за допомогою біометричних інструментів є результатом використання загальної стратегії, в рамках якої зображення, отримане за допомогою різних сенсорів, передається до біометричної системи. Після цього система проводить порівняння вхідного зображення з базою даних за допомогою спеціального алгоритму та виводить результати процедури розпізнавання. Класифікація типів біометрії зазвичай розподіляється між двома основними категоріями: біологічна біометрія та поведінкова біометрія (Рис. 1.2).

Біологічна біометрія зосереджується на аналізі розміру, форми та біологічних особливостей людського тіла. Цей розділ можна розглядати як великий спектр ідентифікаційних методів, що базуються на унікальних біологічних характеристиках кожної особи. Широкий спектр біологічних даних включає в себе візуальну, хімічну, нюхову, просторову та інші категорії.

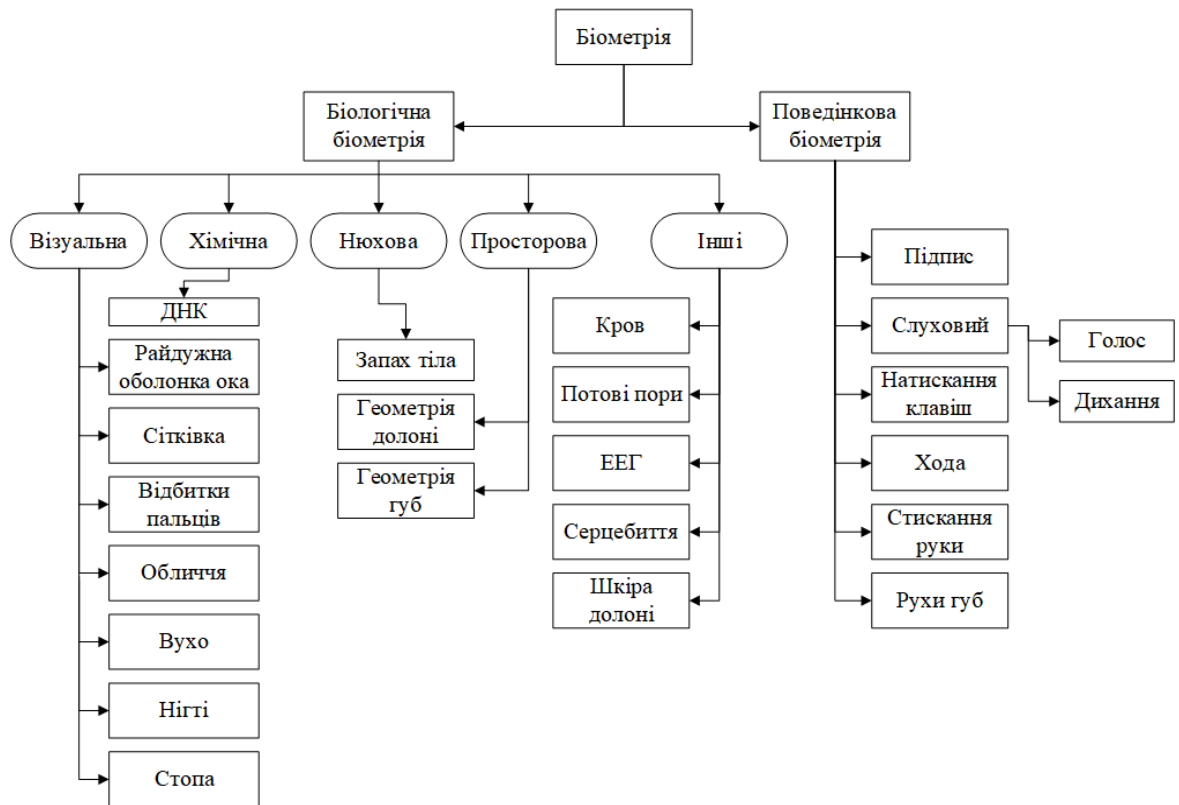


Рис. 1.2. Категорії біометрії

1.2.1 Візуальна біометрія

Класифікація біометричних методів у візуальній біометрії визначається органами тіла людини, які можна побачити очима.

Райдужна оболонка ока виконує ключову роль у системі біометричного розпізнавання, забезпечуючи важливу інформацію для ідентифікації особи. Ця унікальна біометрична характеристика є так само індивідуальною, як і відбитки пальців, і навіть в однайцевих близнюках райдужні оболонки відрізняються.

Один із методів біометричної ідентифікації, що базується на райдужній оболонці ока, включає аналіз дайджесту райдужної оболонки з використанням вектора ознак та розробку біометричного ідентифікатора [14]. Поширена біометрична система на основі райдужної оболонки ока включає в себе сканер, який зафіксує зображення райдужної оболонки, й аналізатор, що оптимізує зображення, мінімізуючи вплив вії.

Виразні характеристики райдужної оболонки виникають внаслідок випадкового розподілу ознак, роблячи цей метод високонадійним для

ідентифікації особистості [15, 16]. Зростання акценту на безпеку призвело до широкого застосування автоматичної ідентифікації осіб, де розпізнавання за райдужною оболонкою ока відіграє ключову роль.

Системи розпізнавання райдужної оболонки ока знаходять застосування в різних областях, таких як паспортні та національні системи посвідчення особи. Рисунок 1.3 ілюструє систему розпізнавання райдужної оболонки ока, що стає динамічною темою досліджень та практичних застосувань.

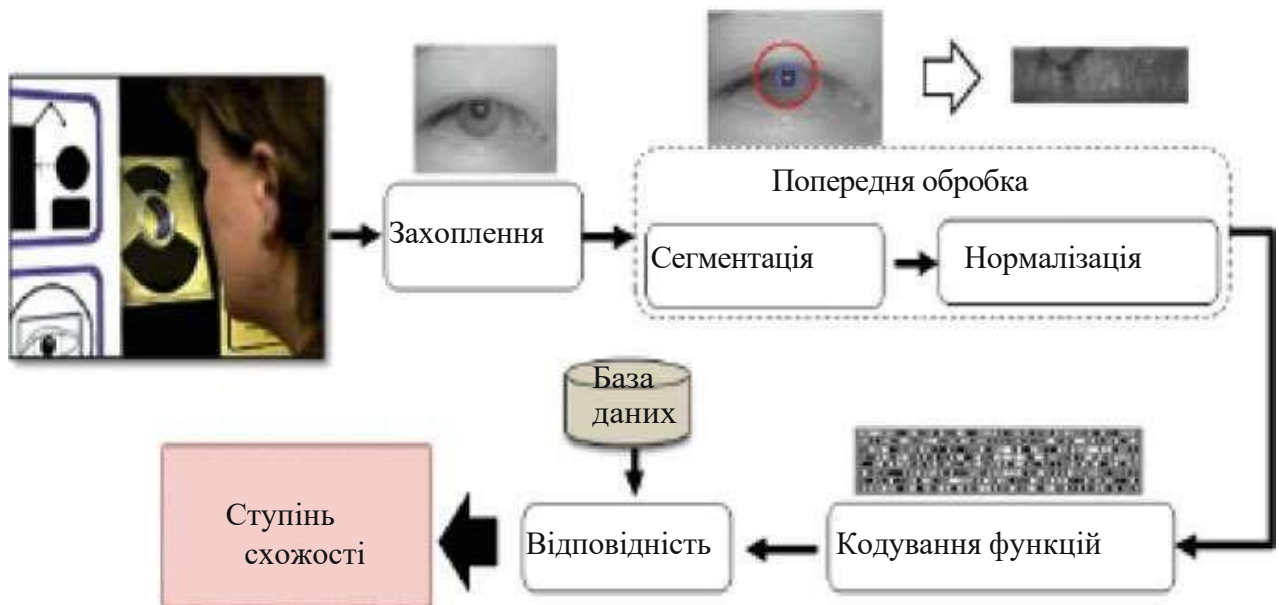


Рис. 1.3. Система розпізнавання райдужної оболонки ока [17]

Сітківка ока, важлива складова зорової системи людини, володіє не лише винятковим значенням для процесу бачення, але й може служити ефективним інструментом для ідентифікації особи за її унікальною структурою кровоносних судин. Ця структура є індивідуальною для кожної людини, якщо не має втрат чи захворювань. Зокрема, цифрове зображення сітківки може бути застосоване для автоматизованої ідентифікації особи шляхом порівняння зображення сегментованих кровоносних судин сітківки з попередньо записаним зразком [18].

Біометрична ідентифікація на основі сітківки ока визначається високою надійністю та точністю, роблячи її однією з найефективніших систем автентифікації після ДНК [19]. Важливим аспектом використання цієї технології є низька ймовірність помилок і доступність цифрових камер для

зйомки зображення сітківки, що робить її не тільки високоефективною, але й економічно вигідною.

Системи біометричної безпеки за відбитками пальців (FPBSS) представляють сучасні рішення для персональної ідентифікації, використовуючи фізіологічні особливості людини. Ці системи, відомі як біокриптосистеми [20], націлені на забезпечення безпеки шляхом збереження та порівняння шаблонів. Вони використовують уні-біометрію та мульти-біометрію для забезпечення високого рівня безпеки й точності ідентифікації і розпізнавання особи.

У випадку уні-біометрії FPBSS виявили обмеження в точності та безпеці. Сучасні вимоги безпеки ведуть до інтенсивного використання мультибіометричних систем, які використовуються для розпізнавання осіб в різних галузях безпеки.

У системах біометричної безпеки з об'єднаним відбитком пальця використовуються як відбитки пальців, так і вени пальців для створення унікального шаблону. Цей шаблон оцінюється та захищається для подальшого використання в інших системах. Однак нещодавно системи FPBSS почали стикаються з викликами, пов'язаними зі зіставленням шаблонів при скануванні бічних та неповних відбитків пальців [21]. Проблеми, такі як підробка шаблонів та вразливість злитих шаблонів для узагальненого зіставлення, стають великими викликами в області систем зіставлення відбитків пальців та біометричної безпеки.

На сьогоднішній день дослідники активно працюють над розробкою моделей, які практично впроваджуються з метою поліпшення точності та безпеки систем в біометрично захищеному середовищі. Це вказує на постійний прогрес у вдосконаленні технологій біометричної безпеки та розвитку нових методів для забезпечення найвищого рівня захисту в цифровому світі.

Розпізнавання обличчя є поширеним видом біометрії [22-28], що зосереджується на найбільш чіткому ідентифікаторі людини – її обличчі. Замість того, щоб чекати, коли людина наведе руку на сканер або детально підведе очі до пристрою для зчитування, біометрична система невидимо

фотографує обличчя особи. Цей процес відбувається непомітно, і зазвичай люди не мають уявлення про те, що їх фотографію знімають, та не відчують себе під наглядом.

Розпізнавання обличчя – це широко відома біометрична технологія [29-32], яка застосовується в різних галузях, пов'язаних із безпекою та спостереженням. Такі застосування включають міжнародну ідентифікацію, посвідчення особи, розвідку в реальному часі та інші.

Процес розпізнавання обличчя включає попередню обробку зображення, що може включати в себе стандартизацію, зміну розміру та ідентифікацію. Після цього оброблене зображення обличчя порівнюється з базою даних для визначення особи [33]. Елементами, що впливають на процес розпізнавання, є різновиди поз, освітлення, можливі перешкоди та інші фактори, які враховуються для досягнення точності та ефективності системи [34-38].

Біометрія вуха – цей термін вказує на автоматичне розпізнавання особи на основі характеристик вуха, фізіологічних за своєю природою. При цьому враховуються різноманітні функції, що зазвичай визначаються на основі двовимірних або тривимірних зображень.

Параметри вуха, використовувані в процедурі ідентифікації, включають геометричну форму вуха, характерні кінчики вух, універсальні та локальні функції візуалізації вуха, а також тривимірні моделі [39]. Важливо відзначити, що вуха не є структурами, які зазнають випадкових змін, вони відрізняються за своєю природою від інших біометричних особливостей, таких як обличчя, тим, що не змінюють колір і вираз, і не піддаватимуться впливу макіяжу.

Процес розпізнавання обличчя включає в себе попередню обробку зображення, стандартизацію, зміну розміру та ідентифікацію, а після цього порівнює оброблене зображення з базою даних для визначення особи. Однак залишається відкритим питання, чи можна вважати вухо унікальним для використання в біометрії, а також якісь деталі стосовно його неперевершеності і стабільності протягом життя.

Останні дослідження в галузі будови вуха працюють над тим, щоб визначити його унікальність і постійність, що відкриває нові можливості використання вуха як надійної біометричної характеристики[40]. Відмінною особливістю вушної біометрії є те, що цей метод виглядає більш природним порівняно з іншими техніками, такими як сканування обличчя чи відбитки пальців. Перевагою є те, що не потрібно виконувати складні рухи або витратити зусилля на спрощені процедури верифікації, навіть при невеликих рухах.

Отже, вухо володіє усіма необхідними біометричними характеристиками, такими як унікальність, довговічність і різноманітність, і відображає збільшену зацікавленість в його використанні в сучасних системах аутентифікації [41].

Ніготь на пальці є унікальним джерелом біометричних даних, які можуть служити важливим інструментом для ідентифікації особи [42]. Цей метод біометричної верифікації вважається одним з найбільш надійних і безпечних. Оскільки дані з нігтя неможливо просто скопіювати, вони можуть ефективно використовуватися для індивідуальної ідентифікації, аутентифікації для забезпечення безпеки, доступу до банківських рахунків, а також для участі в ключових подіях та інших заходах.

Біометричні дані, що знаходяться на нігті пальця, можуть бути зчитані за допомогою лазерного імпульсу Femto. Отримані дані зберігаються в базі даних та порівнюються з інформацією, отриманою під час активування, для підтвердження авторизації користувача.

Цей метод видається надійним у порівнянні з іншими біометричними технологіями, такими як відбитки пальців чи розпізнавання обличчя. Відбитки пальців можна легко скопіювати, а обличчя може бути відтворене за допомогою різних програм редагування зображень. У випадку райдужної оболонки ока, хоча вона є унікальною, її можна пошкодити, зробивши інформацію менш надійною. ДНК є найбільш безпечним методом, але вимагає багато часу і складних процедур.

Відбиток нігтя, хоча подібний до відбитка пальця, є трошки складнішим, що робить його найбільш надійним для забезпечення правильної ідентифікації. Такий метод виявляється безпечним та ефективним в застосуванні для

збереження особистої безпеки й виключення можливості несанкціонованого доступу.

Визначення особи за відбитком стопи представляє собою ще одну біометричну характеристику [43]. Розпізнавання особи здійснюється на основі форми та візерунків відбитків ніг. Цей метод є легким у фіксації, універсальним та статичним зі зміною в часі. Однак в деяких випадках його використання може бути незручним, оскільки вимагає наявності зображень босих ніг [44].

Процес ідентифікації починається з нормалізації необроблених вхідних зображень обох стоп у напрямку орієнтації та положення. Після цього порівнюється оброблене вхідне зображення з зареєстрованим відбитком стопи. Проте, іноді під час нормалізації може бути втрачена корисна інформація. З метою уникнення цієї проблеми, геометрична інформація вхідних зображень пари враховується в оціночній функції перед нормалізацією.

Ідентифікація особи за відбитком стопи представляє собою важливий біометричний метод, який може бути використаний в різних областях, таких як безпека та контроль доступу. Враховуючи його унікальність та стабільність з часом, цей метод може забезпечувати надійний засіб ідентифікації особи без необхідності спеціальних обладнань чи складних процедур.

1.2.2 Хімічна біометрія

Хімічна біометрія включає в себе аналіз хімічного складу Дезоксирибонуклеїнової кислоти (ДНК) людини, що є основою для визначення її ідентичності [45].

ДНК є складовою кожної клітини організму людини та містить важливу генетичну інформацію. Складаючись з чотирьох основ (аденін, гуанін, цитозин, та тимін), ДНК утворює пари, які утримують генетичний код. Сучасна наука визнає ключову роль ДНК у вирішенні питань безпеки та ідентифікації особи.

Сьогодні ДНК використовується як потужний інструмент для визначення особистої інформації. У справах кримінального розслідування, ДНК може служити ключовим елементом для ідентифікації злочинців. Судово-медичні

експерти взямають зразки з місця злочину, такі як кров, волосся чи нігті, для отримання клітин, які містять ДНК. Завдяки тому, що ДНК є унікальним для кожної особи, вона дозволяє точно провести ідентифікацію [46].

Нюхова біометрія

Біометричні методи, пов'язані із запахом людського тіла, представляють собою інноваційний напрямок, що привертає увагу вчених. Запах тіла виникає внаслідок бактеріальної активності, спричиненої певними шкірними залозами. Унікальний хімічний склад летючих сполук (Volatile Organic Compounds, VOCs), який міститься в запаку тіла, надає можливість легко визначати стан організму людини [47].

Запах тіла містить безліч стійких та індивідуальних патернів, що робить його ідеальним для біометричного розпізнавання. Унікальна будова тіла кожної людини дозволяє впізнавати особу навіть в густо населеному середовищі. В порівнянні з іншими біометричними методами, такими як райдужна оболонка ока та відбитки пальців, розпізнавання запаху тіла не має схильності до відмов користувачів і відзначається високою ефективністю.

Ідея використання запаху тіла для розпізнавання не нова і вже протягом десятиліть використовується силовими структурами та мисливськими собаками [48]. Мисливські собаки, яких навчають відмічати індивідуальний запах злочинця, служать відмінним прикладом успішного використання цього підходу. Інші дослідження запаху тіла вказують на його величезний потенціал як ефективного інструменту для біометричного розпізнавання. Інтерес до цього методу зростає, і він може стати ключовим компонентом у розробці сучасних систем ідентифікації особи.

1.2.3. Просторова біометрія

Біометричні методи, що базуються на геометричних формах органів тіла, визначаються їх просторовими характеристиками.

Геометрія руки представляє собою ефективний метод біометричної ідентифікації, який використовує форму та структуру долоні для розпізнавання

користувача. Цей метод вважається одним з найнадійніших для персональної ідентифікації, оскільки форма рук і долонь містить велику кількість унікальних характеристик. Кожна особа має власну форму долоні та унікальний візерунок ліній, які залишаються сталими протягом усього життя.

Сканер геометрії долоні спершу визначає розміри долоні та лінії, а потім порівнює ці виміри з вже збереженими в системі. Цей метод ідентифікації є надзвичайно точним, бо враховує різноманіття геометричних параметрів долоні.

Іншим аспектом просторової біометрії є **геометрія губ**, яка включає в себе висоту, ширину, контур та центр губ [49]. Ці геометричні характеристики розглядаються як елементарні компоненти для ідентифікації особливостей обличчя та губ. Об'єднання рис обличчя і губ забезпечує підвищену точність ідентифікації, а також зниження ризику помилок.

Інші біологічні біометричні дані

Розглянемо додаткові біометричні параметри, які входять в цю категорію:

Ідентифікації особи за допомогою візерунків кров'яних вен є вельми актуальним та популярним у наше сучасне період. В організмі людини існують взаємопов'язані кровоносні артерії, які утворюють величезну мережу візерунків вен, використовуваних для безпечної біометричної ідентифікації. Унікальність та відмінність візерунків вен кожної особи роблять їх ефективним ідентифікатором, при цьому цей біометричний параметр залишається непомітним озброєному оку. Зокрема, візерунок вен на пальцях і тильній стороні долоні вважається більш безпечним і менш схильним до помилок порівняно з іншими методами ідентифікації.

У сучасних системах біометричної безпеки основний акцент робиться на використанні візерунків вен пальців. Для виявлення візерунка вен пальця, спочатку здійснюється зафіксування зображення за допомогою інфрачервоних променів, що відображає найдрібніші та точні деталі вен [50]. Біометрична система також використовує тильну поверхню долоні як ключовий компонент для забезпечення безпеки. Визначальним є використання пристроїв, що

отримують зображення за допомогою інфрачервоного світла. Після отримання зображень, головною метою є екстрагування важливої інформації та ознак для подальшого аналізу. Виділення ознак за їх формою виявляється дуже ефективним методом, оскільки геометричні характеристики дають обсяг інформації щодо структури вхідного зображення [51].

Останні дослідження акцентують увагу на гібридному підході до системи біометричної автентифікації, який поєднує тильну сторону долоні та візерунки вен на пальцях [52].

Біометричний аналіз потових пор. Ще в 1912 році Е. Локар вивчав структуру потових пор і визначив, що їхня кількість та форма можуть служити основою для ідентифікації. Зазначено, що від 25 до 45 пор є достатніми для визначення особи. Ці пори можуть бути використані як унікальний біометричний параметр. Важливо відзначити, що кількість пор на дюйм може варіюватися від 10 до 19 та від 23 до 46 [53].

Для відображення пор поту використовуються гідрохромні матеріали. Ці матеріали дозволяють не лише відобразити пори чітко, але й ідентифікувати різницю між активними та неактивними порами [54]. Гідрофільна полімерна плівка також використовується для мапування потових пор. На цій плівці пори утворюють виразні мікроямки, що дозволяють використовувати цей метод для біометричної ідентифікації.

Ще однією перспективною методикою є використання алгоритмів обробки зображень, які базуються на нейронних мережах [55]. Ці алгоритми забезпечують точне виділення потових пор із сукупності точок-конкурентів. Додатково, алгоритм, заснований на геометричних перетвореннях і методах двосторонніх графів, допомагає у визначенні пор і є унікальним у тому, що підвищує продуктивність систем ідентифікації за відбитками пальців [56]. Біометрична система, що використовує аналіз потових пор, включає датчик, що генерує зображення, що містить інформацію про пори потових залоз.

Сигнал електроенцефалограми (ЕЕГ). В останні роки збільшилось зацікавлення наукової спільноти у використанні сигналів мозку для

автоматичного розпізнавання осіб. Традиційні методи біометрії, такі як розпізнавання обличчя, відбитків пальців чи райдужної оболонки ока, поступово витісняються сучасними технологіями, такими як ЕКГ, EDR і BVP. Ці нові підходи виявили значні переваги, забезпечуючи високий рівень захисту і ускладнення можливості підробки.

Аналіз сигналів мозку, отриманих за допомогою ЕЕГ, виробляє активність із високою часовою роздільною здатністю, і це досягається за допомогою доступних і ефективних пристроїв [57]. Завдяки протоколам реєстрації вивчають різноманітні електричні активності мозку, що визначаються різними станами та діями.

Проте, однією з основних труднощів у використанні ЕЕГ-біометрії є наявність шуму в отриманих даних. Цей шум може бути спричинений активністю м'язів (ЕМГ) та імпедансом електродів [58]. Вирішення цієї проблеми стає ключовим завданням для подальшого вдосконалення точності та ефективності систем автоматичного розпізнавання осіб на основі сигналів ЕЕГ.

Серцебиття. Важливим фізіологічним сигналом в організмі людини є звуки серця, які несуть в собі ключову інформацію про фізіологічний стан особи. Ця цінна інформація взаємодіє з даними від шлуночків, передсердь, головних артерій та функціонального стану клапанів. Під час перекачування крові серце генерує звук або вібрацію, відому як фонокардіографія [59].

Факт того, що людське серце генерує унікальні звуки серцебиття, наводить на думку про використання цього сигналу в біометричних системах. Висока ступінь універсальності цього методу обумовлений тим, що тіло не може відтворити серцебиття, забезпечуючи можливість автентифікації живих і неживих об'єктів. Така особливість може бути використана для ідентифікації важливих органів, зокрема мозку, функції якого є критично важливими.

Незважаючи на переваги, існує важливий недолік у використанні серцебиття як біометричної ознаки, а саме його обмежена презентація. Тривалість часу, протягом якого можливо зафіксувати цей сигнал, може бути

обмеженою, що становить виклик для визначення його ефективності в біометричних системах.

Біометрія шкіри пальців рук. Одним із широко використовуваних методів ідентифікації особи є розпізнавання вен на долоні, що забезпечує високий рівень безпеки. Візерунок вен, знаходячись під шкірою, залишається невидимим для людського ока, а його захоплення можливе лише за допомогою сенсорного пристрою, що використовує інфрачервоне випромінювання [60].

Найзначущою перевагою долонної вени є її стабільність, оскільки візерунок вен залишається незмінним протягом усього життя людини, а його модифікація є практично неможливою. Три шари шкіри - епідерміс, внутрішня дерма і підшкірна клітковина - утворюють складну структуру, що складається з артерій, жирових тканин і кровоносних судин у різних пропорціях.

Використання інфрачервоних датчиків для отримання візерунку вен дозволяє виявляти лише справжню кров, ускладнюючи можливість підробки. Інфрачервоне випромінювання проникає крізь тканини шкірного покриву, які блокують пігменти, такі як гемоглобін. Густа мережа кровоносних судин, що складається з гемоглобіну, призводить до того, що венозний блиск на вихідному зображенні з'являється у вигляді темних тіньових контурів.

Такий технологічний підхід не лише підвищує безпеку, а й робить біометрію вен на долоні надзвичайно надійною та важкодоступною для шахрайства.

1.3 Об'єкти й технології поведінкової біометрії

У цьому напрямку біометричні технології охоплюють різноманітні аспекти, такі як підпис, голосове визначення, динаміка натискання клавіш, хода і хват руки. Ці варіації біометричних характеристик засновані на

індивідуальних особливостях побутової поведінки, що робить їх унікальними для кожної людини.

Підпис. Розпізнавання або верифікація підпису представляє собою важливий аспект поведінкової біометрії, який використовується для ідентифікації особи [61-63]. Це фізична дія, що дозволяє встановити особу на основі її підпису. В цьому контексті існують два основних методи вивчення особи: статичний і динамічний.

У статичному методі особа подає власноручний підпис, який зафіксовується з використанням сканера або камери. Зображення підпису перетворюється в текстові або інші формати для подальшої перевірки. Цей метод також відомий як офлайн-перевірка підпису. Застосування різних алгоритмів обробки зображень та машинного навчання дозволяє ефективно перевіряти автентичність підпису.

Динамічний метод пов'язаний із передовими технологіями, де особи використовують смартфони, планшети чи КПК для створення підпису пальцем або стилусом. Індивідуальні особливості підпису, такі як напрямок, штрих, тиск і форма, фіксуються та перевіряються. Динамічна перевірка підпису має важливу перевагу – практично повна неможливість його повторення і легке виявлення підробки.

Використання високоточних методів обробки даних та алгоритмів робить біометрію підпису ефективним і безпечним засобом ідентифікації особи.

Слуховий. У категорії аудіальної біометрії вирізняються різноманітні слухові дані, серед яких особливо важливими є голос та дихання.

Голосова біометрія представляє собою ефективний метод ідентифікації особи, оцінюваний як найкращий біометричний інструмент за результатами дослідження Unisys. Цей метод може використовуватися в областях високочутливої безпеки, де необхідно надійне розпізнавання. Розпізнавання голосу надає унікальну можливість ідентифікації особи, особливо в ситуаціях, коли доступні лише аудіозаписи голосу.

Сучасні методи розпізнавання мовлення, такі як Мел-частотні кепстральні коефіцієнти (MFCC) [64], використовуються для точного розпізнавання мовця за його голосом. Додатково, алгоритми на основі вейвлет-аналізу та глибокого навчання визнані як більш точні у розпізнаванні дикторів [65]. Використання розпізнавання голосу розповсюджене у сферах оборони, правоохоронних органів, ділової взаємодії, колл-центрів, криміналістики і безпеки.

Дихання, як біометрична характеристика, виявляється унікальною та ефективною для однозначної ідентифікації особи. Це анатомічне діяння, що контролюється різними фізіологічними елементами внутрішньолегеневого тиску, голосових шляхів, дихальних м'язів та органів дихання [66].

Дихання може служити відмітною біометричною характеристикою через його вплив на внутрішні мікроорганізми організму людини. Методи, які використовують звуки дихання для ідентифікації, засновані на піднятті мікрофонного датчика ближче до носа людини.

Дихання, як біометричний параметр, може знайти застосування у медичній діагностиці, моніторингу вживання ліків, а також в області антидопінгових заходів у спорті. У повітрі, що видихається містяться характерні сполуки, які можуть слугувати як молекулярний відбиток дихання, що залишає стійкий слід для верифікації та моніторингу здоров'я.

Дихальна біометрія, як додатковий вид ідентифікації, відзначається своєю універсальністю та здатністю працювати без додаткових фізичних чи когнітивних зусиль [67].

Динаміка натискання клавіш - це біометричний метод, який використовується для автентифікації особи та розрізняє їхній унікальний стиль набору тексту [68, 69]. Цей нестатичний підхід визначається динамікою та часовими параметрами натискання клавіш.

Прогресія натискання клавіш - це точкові хронометричні дані, які точно відображають моменти натискання та відпускання кожної клавіші під час введення тексту на комп'ютерній консолі. Інформацію щодо часу натискання

клавіш обробляє алгоритм, який визначає важливі зразки для майбутньої автентифікації.

Біометрична система для динаміки натискання клавіш складається з трьох основних етапів: збір даних, виділення ознак і картування. Цей метод відрізняється простотою впровадження, не потребує додаткового обладнання, крім комп'ютерної консолі, легко передається і використовується кінцевим користувачем.

Незважаючи на переваги, такі як висока ефективність та зручність в застосуванні, динаміка натискання клавіш має свої недоліки, такі як вразливість до втоми користувача, можливість динамічних змін у стилі письма, можливість травм та вимога до періодичного оновлення консольного обладнання.

Хода, або стиль ходи людини, є унікальним біометричним методом, що може бути використаний для ідентифікації особи [70]. Результати багатьох фізіологічних досліджень підтверджують, що кожна людина має свій власний, важко копіюємий стиль ходи. У свою чергу, хода відіграє значущу роль у відеоспостереженні для забезпечення безпеки та розшуку людей, оскільки може бути зафіксована з відстані за допомогою кількох камер та під різними кутами, навіть у щільно населених місцях.

Однією з ключових переваг ходи як біометричної характеристики є її безконтактний характер, що робить збір даних більш ефективним [71]. Однак існують фактори, що впливають на процес розпізнавання ходи, такі як умови перенесення, одяг, вплив освітлення, тіні під ногами і швидкість ходьби [72].

Для подолання цих проблем розроблено різноманітні методи. Одним із них є підхід, заснований на моделях, який використовує структуру людського тіла для відстеження руху з розрахунком кутів нахилу суглобів. Цей метод, відомий як інваріантний вигляд і масштаб, відзначається високою інформативністю, хоча вимагає високоякісного відео для визначення ознак. Ще один підхід, названий підходом на основі зовнішності, використовує силует людини для виділення корисних ознак та аналізує просторово-часову структуру ходи [73].

Крім того, для біометричної ідентифікації ходи застосовують підлогові датчики та мікроелектромеханічні системи (MEMS), розташовані в тілі або на "розумному" взутті [74]. Ці сучасні методи забезпечують точність та ефективність у визначенні індивідуального стилю ходи людини.

Стискання руки, або сила кистьового хвату, визначається як здатність руки утримувати предмет. Цей параметр може служити не лише мірою фізичного стану людини, але і важливим фактором для оцінки загального здоров'я та харчування. Сила кистьового хвату безпосередньо пов'язана з різними фізичними характеристиками, такими як вік, стан здоров'я та інші. Змінюючи вагу предмета, який потрібно схопити, можна виміряти, наскільки сильним є хват руки.

Дієтологи та медичні фахівці використовують силу кистьового хвату як інструмент для виявлення пацієнтів із недоїданням [75]. Збираючи дані про силу хватки руки, можна визначити не тільки структуру руки, але й її поведінку під час стиску. Цей біометричний показник є важливим для моніторингу змін у стані здоров'я та динаміки захворювань.

Для вимірювання сили кистьового хвату використовують електронні динамометри, наприклад, Jamar. Ці пристрої дозволяють виміряти силу кистьового хвату з урахуванням різних параметрів, таких як тренованість, довжина кисті, сила індивіда тощо. Динамометри Jamar широко застосовуються у клінічній практиці, хоча вони є однонапрямковими [76].

Для виявлення вогнепальної зброї використовуються датчики COTS, які є малопотужними та недорогими. Однак розробка повноцінної системи виявлення залишається завданням, що потребує подальших досліджень [77].

Висновки до розділу 1

Встановлено, що біометрія є синтезом технологічних і наукових методів автентифікації, заснованих на біологічних особливостях людини, які сьогодні широко застосовуються в галузі IT та безпеки. Використання унікальних фізичних і поведінкових характеристик особи забезпечує високу надійність методів ідентифікації, що перевершують традиційні методи із застосуванням паролів чи карток доступу.

Аналіз розвитку біометричних технологій показав, що на їх вдосконалення та розповсюдження позитивно вплинули стандартизація, розвиток апаратних засобів і зростання потужності обчислювальної техніки. Ці фактори взаємодіють для забезпечення успішного впровадження біометричних технологій і визначають їхню важливу роль у сучасних системах ідентифікації.

Біометричні технології поділяють на дві групи: біологічну й поведінкову. Біологічна біометрія, яка базується на фізіологічних та біологічних характеристиках організму, є однією з найперспективніших із біометричних технологій. Враховуючи унікальність і стійкість біологічних параметрів, таких як відбитки пальців, розпізнавання сітківки ока й обличчя, ці технології не лише дозволяють ефективно вирішувати завдання ідентифікації, але й знаходять застосування в різних галузях, включаючи безпеку, медицину тощо.

Аналіз показав, що за останні роки значно зріс інтерес до технологій поведінкової біометрії, які базуються на ідентифікації індивідуальних особливостей, таких як манера ходьби, письма, спосіб введення тексту на клавіатурі тощо. Застосування поведінкових біометричних даних не лише забезпечує додатковий рівень безпеки, але й відкриває шлях до зручних і непомітних систем ідентифікації. Із врахуванням стрімкого технологічного розвитку та підвищення вимог щодо захисту конфіденційності даних, поведінкова біометрія може стати ключовим елементом у вдосконаленні безпеки та зручності в цифровому світі.

РОЗДІЛ 2

ОСОБЛИВОСТІ Й ПЕРЕВАГИ СИСТЕМ МУЛЬТИМОДАЛЬНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

2.1 Загрози і вразливості біометричних систем та їх захист

У сфері біометричних систем виділяють два основні типи неполадок. По-перше, внутрішні збої, які пов'язані з обмеженнями у апаратному або програмному забезпеченні і виникають безпосередньо без зовнішнього втручання. По-друге, збої, ініційовані ззовні, виникають тоді, коли зовнішній агент умисно або випадково втручається у функціонування апаратного чи ПЗ, яке використовується в біометричній системі. Атаки на систему можна розділити на фізичні, якщо вони спрямовані на апаратне забезпечення, або системні, якщо вони націлені на ПЗ [78].

Важливо відзначити, що внутрішні збої є результатом внутрішніх обмежень і можуть виникнути внаслідок технічних недоліків чи обмежень ресурсів системи. З іншого боку, зовнішні атаки можуть включати в себе широкий спектр дій, від кібератак до фізичного впливу на апаратне забезпечення.

2.1.1 Типи ворожих атак

Існує багато типів атак зловмисників, найпростіші з яких передбачають безпосереднє маніпулювання біометричним сканером. Однак ці атаки також можуть бути атаками на програмне забезпечення.

Інсайдерські атаки

Цей вид атак виникає внаслідок будь-яких витоків чи маніпуляцій із боку осіб, які мають прямий доступ або контроль до біометричної системи. Такі атаки можуть бути випадковими, наприклад, коли власник системи не перевіряє

облікові дані потенційного користувача. З іншого боку, інсайдерські атаки можуть бути наслідком умисного надання неавторизованим особам доступу або втручання авторизованого користувача у роботу системи.

Важливо зазначити, що цей вид атак часто виходить за межі технічних рішень, оскільки він пов'язаний з управлінням персоналом і внутрішніми процедурами.

Біометрична відкритість

Ця атака спрямована на обман біометричного сканера, змушуючи його помилково ідентифікувати користувача як авторизовану особу. Такі атаки можуть включати в себе використання високоякісних відбитків пальців, моделювання очного яблука або імітацію ходи особи.

Незважаючи на те, що ця проблема є серйозною, вона також вважається однією з найбільш вирішуваних у сфері безпеки біометричних систем.

Незахищена інфраструктура

Цей тип атак включає будь-які маніпуляції з даними, які передаються на будь-якому етапі процесу автентифікації після здійснення біометричного сканування. Ці атаки часто пов'язані з пошуком вразливостей у безпеці баз даних, де зберігаються автентифікаційні дані користувачів, або самій структурі даних, такій як слабе шифрування.

2.1.2 Захист апаратного забезпечення

Існує ряд ефективних стратегій для протидії фізичним атакам на біометричні сканери, важливих для забезпечення високого рівня безпеки системи. Розглянемо декілька методів:

Фізична безпека

Один з підходів до захисту біометричного сканера полягає в посиленні його фізичного захисту. Це може включати розміщення спостерігачів або встановлення камер, які контролюють область сканера. Додатковий рівень безпеки може бути досягнутий вимаганням пароля для доступу до самого

сканера. Однак варто враховувати, що ці заходи можуть суперечити основній меті біометричної ідентифікації та не рекомендуються.

Захист сканера

Ефективніше може бути ускладнення самого біометричного сканера. Для захисту від фальшивих відбитків пальців або сканування сітківки ока можна використовувати тепловий датчик, який визначатиме автентичність представленого пальця або очного яблука [79]. Наприклад, сканер підпису може включати сенсорну панель, щоб впевнитися, що користувач не намагається відтворити чужий підпис.

Ці підходи дозволяють підняти планку безпеки біометричних сканерів та забезпечити надійний рівень захисту від фізичних атак.

2.1.3 Надійне зіставлення відбитків пальців

Шенлін Ян (Shenlin Yang) та Інгрід М. Вербауведе (Ingrid M. Verbauwhede) з Каліфорнійського університету в Лос-Анджелесі запропонували метод безпечного зіставлення відбитків пальців [80].

Найчастіше використовуються такі методи: зіставлення на основі зображень, зіставлення на основі графів і зіставлення на основі дрібних деталей. При зіставленні на основі дрібних деталей порівнюються відмінності в деталях відбитків пальців, а не самі відбитки для збігу. До таких деталей відносяться типи присутніх мініатюрних відбитків та їхня відстань один від одного [81].

Дактилоскопічні мініатюри - це незначні деталі відбитка пальця, які відрізняють його від інших відбитків пальців. Основними типами мініатюр є закінчення гребенів, біфуркації гребенів, облямівки гребенів, короткі гребені, острівці, відроги, перехрестя, дельти та серцевини [82].

Зіставлення на основі зображень використовує весь відбиток пальця в сірій шкалі як шаблон для порівняння з іншими відбитками пальців. Цей метод дуже непослідовний, оскільки важко врахувати незначні відмінності. Порівняння на основі графів представляє дрібні деталі відбитків пальців у

вигляді графіків. Однак цей метод має дуже високу обчислювальну складність, що обмежує його практичне використання. Оскільки система зіставлення на основі дрібних деталей використовує більш розбірливі та надійні функції, а також забезпечує вищу швидкість обробки і набагато менший розмір шаблону біометричної інформації, Янг і Вербауде вирішили розробити свою систему на основі зіставлення дрібних деталей.

Алгоритм автентифікації працює шляхом порівняння сусідів мініатюри з сусідами відповідної мініатюри в базі даних. На рис.2.1 наведено приклади мініатюр, сусідами нижнього обведеного островця будуть обведені біфуркація й огороження.

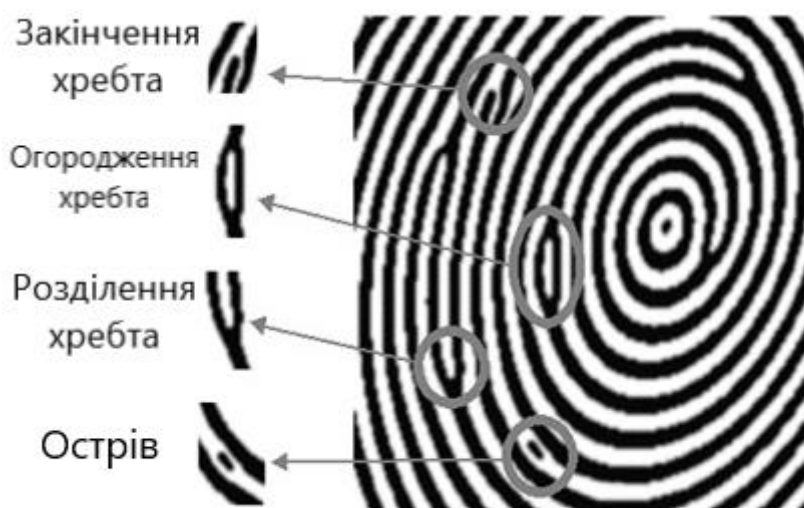


Рис. 2.1. Типи дрібних відбитків пальців.

Як зазначалося раніше, важливою є безпека самих біометричних даних, а не лише сканера. Щоб вирішити цю проблему, деякі біометричні системи намагаються перенести механізми обробки сигналів і зіставлення з сервера на вбудований пристрій (в даному випадку, біометричний сканер). У таких системах біометричні дані обробляються і зіставляються всередині самого сканера, а на сервер надсилається не повний відбиток пальця, а результат обробки і зіставлення. Такий підхід дозволяє уникнути багатьох атак на зв'язок між сканером і сервером, а також на сам сервер.

Однак, скомпрометувати біометричні шаблони, які зберігаються в сканері, відносно просто. Як наслідок, шаблон часто зашифрований. Коли

надходить запит, для декодування шаблону використовується ключ шифрування, який потім використовується для обробки вхідних даних. Цей ключ може бути вилучений шляхом аналізу зовнішніх ефектів, таких як синхронізація, електромагнітне випромінювання та енергоспоживання. Такий тип атаки називається атакою побічного каналу (Side Channel Attack, SCA), а найпоширенішою формою SCA є аналіз диференціальної потужності (Differential Power Analysis, DPA). DPA - це атака, яка відстежує енергоспоживання пристрою і може виявити збіг за різним енергоспоживанням. SCA найбільш ефективні проти портативних пристроїв, оскільки на них часто не вистачає місця, щоб додати надлишкову обробку даних, яка може бути використана як шум, щоб обдурити злоумисника.

Система Янга і Вербауведе вирішує цю проблему, розбиваючи процес на дві частини: незахищену частину і захищену частину, яка працює на платформі, захищеній від DPA. Все, що позначено сірим кольором на рисунку 2.2, знаходиться в захищеній частині, тоді як все, що не позначено сірим кольором, знаходиться в незахищеній частині.

Для протидії витoku інформації з захищеної частини використовується логіка на основі підсилювача чутливості (SABL), яка відповідає за зберігання та обробку вищезгаданих даних. SABL розроблена з постійним енергоспоживанням та іншими методами, щоб зупинити витік інформації з побічних каналів.

З розвитком технологій SCA, а особливо DPA, почали застарівати. Однак метод, який Янг і Вербауведе використовували для боротьби з ними, все ще актуальний. Як і багато інших, Янг і Вербауведе використали метод хешування на додаток до SABL, щоб ще більше знизити ефективність DPA. Однак хешування є дуже ризикованим у біометрії, оскільки деякі біометричні дані відбитків пальців можуть змінюватися залежно від наявності масла або інших косметичних змін, хешування всього відбитка пальця не працює. Щоб вирішити цю проблему, Янг і Вербауведе запропонували алгоритм хешування, який хешує дрібні деталі відбитків пальців, а не самі відбитки. В результаті хеш

може розпізнати найменші деталі кожного відбитка навіть після того, як сам відбиток змінився.

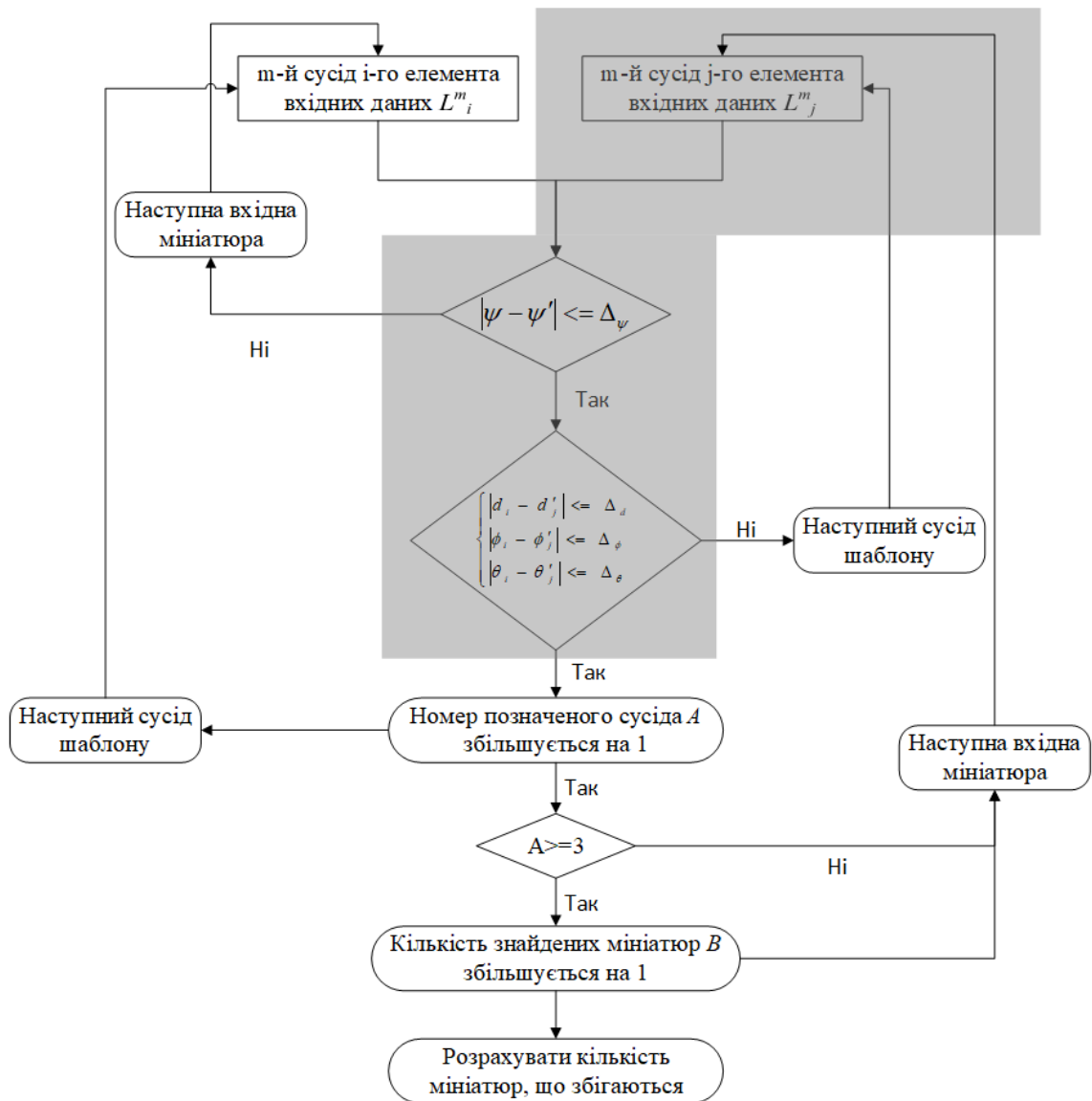


Рис. 2.2. Блок-схема системи зіставлення Янга та Вербауеде.

Детальна інформація про кожну мініатюру M є доступною в результаті збору інформації про оточення M за наступним рівнянням, яке виконується для кожної сусідньої мініатюри

$n \in \{1, 2, \dots, N\}$:

$$\begin{cases} d_n = \sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} \\ \phi_n = \text{diff}(\psi_n, \psi) \\ \theta_n = \text{diff}(\arctan((y_n - y_0)/(x_n - x_0)), \psi), \end{cases} \quad (1)$$

де d_n описує відстань між мініатюрою M та її n^{th} сусідами, ψ_n - відповідний радіальний кут між M та її n^{th} найближчими сусідами, а θ_n - відповідний кут положення n^{th} найближчого сусіда. Позиційний кут - це кутове зміщення сусіда n і мініатюри M , якщо з точки зору провести пряму лінію [83]. Функція $\text{diff}()$ обчислює різницю між двома кутами, а потім переводить результат в діапазон $[0, 2\pi]$. X та y описують положення мініатюр на стандартній шкалі координат.

Алгоритм, який запропонували Янг і Вербауведе, спочатку порівнює напрямки хребтів, на яких базуються мініатюри, відповідно до даного рівняння:

$$|\psi - \psi'| > \Delta_\psi, \quad (2)$$

де ψ має те саме значення, що й у рівнянні 1, а Δ_ψ - це поріг для напрямку хребта, на якому базується мініатюра. Якщо результат менший за поріг, пара відкидається.

Потім алгоритм порівнює околиці мінусів у вхідному відбитку з околицями тих самих мінусів у відповідному відбитку в шаблоні. Якщо мініатюри досить схожі, як визначено рівнянням 3, вони вважаються парою мініатюр, що збігається.

$$\begin{cases} |d_i - d'_j| \leq \Delta_d \\ |\phi_i - \phi'_j| \leq \Delta_\phi \\ |\theta_i - \theta'_j| \leq \Delta_\theta, \end{cases} \quad (3)$$

де Δ_d - поріг для відстані, Δ_ϕ - поріг для радіального кута і Δ_θ - поріг для кута положення.

Загальна кількість пар збігів, які має відбиток пальця після повторення цього процесу на кожній деталі, використовується для обчислення оцінки відбитка пальця наступним чином:

$$S_{core} = B / (\max(K_{input}, K_{temp})), \quad (4)$$

де K_{input} - кількість дрібних деталей у вхідному відбитку пальця, а K_{temp} - кількість дрібних деталей у шаблонному відбитку пальця. Два відбитки вважаються такими, що належать одному пальцю, якщо їхня оцінка перевищує заданий поріг.

2.2 Мультимодальні біометричні системи

З основної гіпотези, що кожен біометричний параметр має свої обмеження, випливає, що розвиток мультимодальних систем є ключовим напрямком вдосконалення сучасних методів ідентифікації. Наприклад, оцінки свідчать, що приблизно 5% населення не мають "розбірливих" відбитків пальців. З цієї точки зору, мультимодальні системи, які використовують кілька незалежних біометричних параметрів, можуть ефективно подолати деякі з цих обмежень.

Мультимодальні системи володіють певними перевагами порівняно з унімодальними. Вони є більш стійкими до хакерських технологій, оскільки підробка кількох біометричних характеристик виявляється складніше, ніж у випадку використання лише одного параметра [84]. Взаємодоповнюючі модальності вводу в мультимодальних системах забезпечують їхню ненадлишковість, надаючи додаткову інформацію. У той час як надлишкові модальності можуть підвищити як точність зібраної інформації, зменшуючи загальну невизначеність, так і надійність системи в умовах зашумленості інформації з однієї модальності.

Вважається, що біометричні системи, які виконують інтеграцію інформації на початковій стадії обробки, демонструють більшу ефективність порівняно з системами, які проводять інтеграцію на пізніших етапах. Оскільки набір ознак містить в собі багатоцільову інформацію про вхідні біометричні дані, порівняно з оцінкою збігу або вихідним рішенням, передбачається, що злиття на рівні ознак приведе до покращених результатів розпізнавання.

Незважаючи на це, на практиці досягнення злиття на рівні ознак може бути важким завданням. Це може впливати з того, що набори ознак різних модальностей можуть бути несумісними, наприклад, власні коефіцієнти обличчя і набір мікронерівностей пальця, і більшість комерційних біометричних систем не надають доступ до наборів ознак або вихідних даних, які використовуються у їхніх продуктах.

Інтеграція різних модальностей і вимірювань від кількох надавачів, є потужним засобом досягнення підвищеної точності й надійності системи [85]. Такий підхід дозволяє використовувати інформацію, отриману від одного біометричного параметра, для покращення розпізнавання в інших модальностях.

У розділі викладено аналіз останніх наукових досліджень у галузі верифікації голосу та обличчя, а також розглянуто аспекти мультимодальної верифікації. Наведено зведені відомості щодо поєднання систем мультимодальної біометричної верифікації, яка включає в себе обличчя та голос, на різних рівнях (див. Рис 2.3).

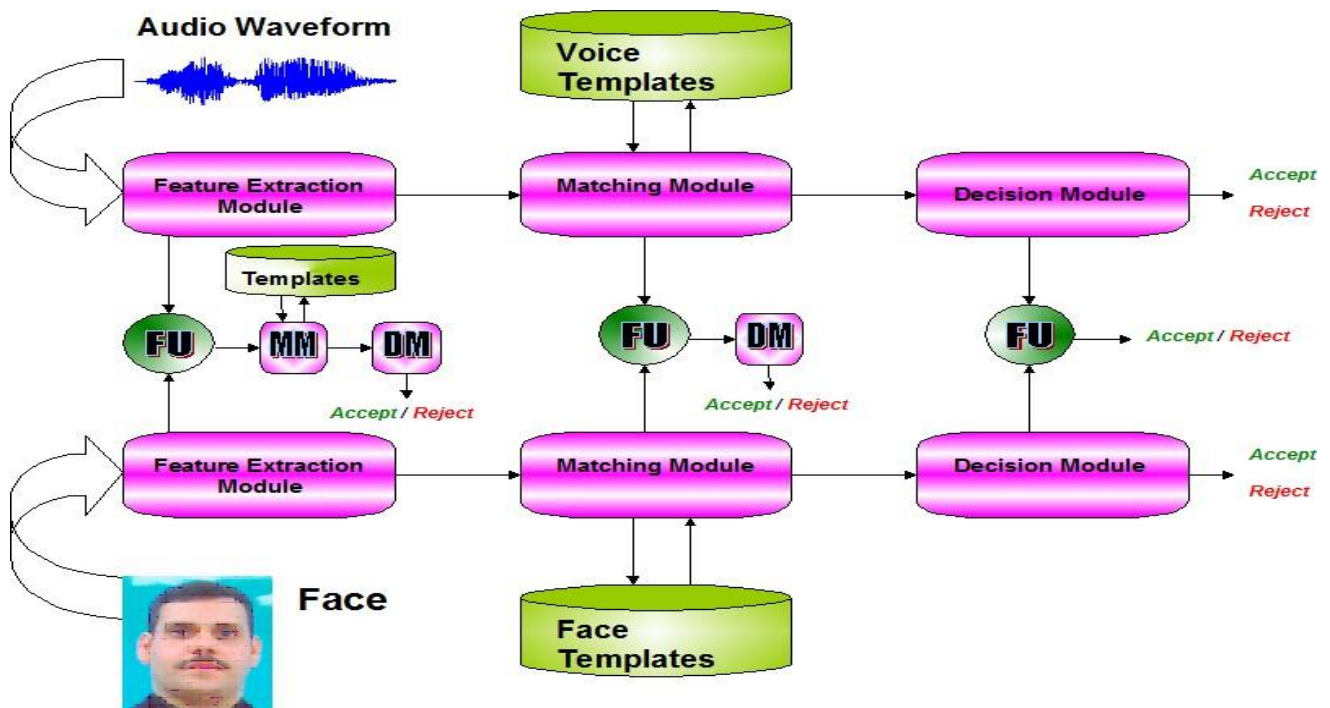


Рис 2.3 Мультимодальна біометрична система, що показує три рівні злиття: FU: модуль злиття, MM: модуль зіставлення і DM: модуль прийняття рішень

2.2.1 Бази даних і протоколи

База даних XM2VTS та Лозаннські протоколи

База даних XM2VTS [86, 87] є цінним ресурсом, що включає синхронізовані відео- та мовленнєві дані, зібрані від 295 учасників під час чотирьох сеансів, проведених із місячним інтервалом. Кожен сеанс включав два записи: мовлення та запис обличчя. Мовленнєвий знімок містив фронтальні зображення обличчя та мовлення для кожного учасника під час промовляння речення.

База даних була розділена на три набори: навчальний (LP Train), оціночний (LP Eval) та тестовий (LP Test). Навчальний набір використовувався для навчання моделей клієнтів, оціночний - для обчислення порогів прийняття рішень та інших гіперпараметрів, а тестовий - для оцінювання продуктивності.

Загалом, 295 учасників були розподілені на групи, зокрема 200 учасників для навчання, 25 для оцінювання та 70 для тестування. Підходи до розділу на навчальні та оціночні групи включають Лозаннський протокол I (LP1) та Лозаннський протокол II (LP2), відмінність між якими полягає у кількості тренувальних знімків на клієнта (три та чотири відповідно).

Важливо відзначити, що LP Eval для обох протоколів використовується для розрахунку оптимальних порогів, які потім використовуються в тестовому наборі LP Test. Результати подані в табл. 2.1 лише для тестових наборів з максимальною нейтральністю й унікальністю (з використанням апріорно вибраного порогу).

В останньому стовпчику представлені терміни, що використовуються у протоколах злиття для бази даних XM2VTS. LP Eval відповідає набору для розробки протоколів злиття, тоді як LP Test відповідає набору для оцінки протоколів злиття.

Таблиця 2.1

Лозаннські протоколи бази даних XM2VTS

Набори даних	Лозаннські протоколи		Протоколи злиття
	LP1	LP2	
LP Train Клієнтські доступи	3	4	-
LP Eval Клієнтські доступи	600 (3×200)	400 (2×200)	Розробка злиття
LP Eval Доступ самозванців	40,000 (25×8×200)		Розробка злиття
LP Test Клієнтські доступи	400 (2×200)		Оцінка злиття
LP Test Доступ самозванців	112,000 (70×8×200)		Оцінка злиття

База даних BANCA

База даних BANCA (Biometric Access Control for Network Applications and E-commerce) [88] була спроектована з метою проведення тестів мультимодальної автентифікації осіб за допомогою різних пристроїв для збору даних (2 камери та 2 мікрофони) та за варіантами сценаріїв (контрольований, погіршений та несприятливий). Зібрано відео- та мовленнєві дані для 52 суб'єктів для п'яти різних мов (англійська, французька, німецька, італійська та іспанська), що включає 26 чоловіків і 26 жінок, загалом 260 суб'єктів. Кожну групу за мовою та гендером розділено на 2 підгрупи (позначені як g1 та g2), кожна з яких складається з 13 осіб.

Кожен суб'єкт брав участь у 12 сесіях запису, кожна з яких включала 2 записи: справжній клієнтський доступ (Т) та інформовану атаку 3 самозванців (І). Графічна частина бази даних включає 5 знімків на один запис. Загалом 12 сеансів були розділені на 3 різні сценарії.

У рамках протоколу BANCA визначається, що справжні записи клієнта для першого сеансу в кожному стані використовуються як навчальний матеріал. У всіх експериментах навчання клієнтської моделі проводилося на трьох записах або менше. Розглядаються два протоколи: Matched Controlled (Mc) та Pooled Test (P). Для Mc одна контрольована сесія використовується для навчання клієнта, тоді як для P ті ж самі контрольовані сесії умов використовуються для тестування клієнта та самозванця.

База даних VidTIMIT

База даних VidTIMIT включає аудіозаписи та відеопослідовності 43 випробовуваних, серед яких 19 жінок і 24 чоловіків. У цій базі даних вони декламують короткі речення, які були взяті з тестової частини корпусу NTIMIT [89, 90]. Зйомки проводились протягом трьох сеансів, з середньою затримкою в тиждень між ними. Такий підхід дозволяє враховувати зміни зовнішності та настрою учасників.

Кожна людина вимовляла десять речень, при цьому перші два речення були однакові для всіх учасників, тоді як решта восьми відрізнялися для кожної особи. Важливо відзначити, що всі сесії включають фонетично збалансовані речення, щоб забезпечити різноманітність і точність даних.

Додатково до записів речень, учасникам також було запропоновано рухати головою вліво, вправо, вгору та вниз. Це дало можливість отримати послідовність поворотів голови, що може бути корисним для аналізу динаміки обличчя та головних рис при вимові.

Деталі щодо біометричних систем, які використовують корпуси VidTIMIT, представлені в [91], де розглядається їхнє застосування та ефективність.

2.2.2 Опис базової системи

Особливості обличчя та мовлення

Експертна система для розпізнавання обличчя базується на ключових характеристиках, які визначають її базовий рівень ефективності:

FN (Face Histogram): FN використовує нормалізоване зображення обличчя, яке поєднується з його RGB-гістограмою. Ця характеристика спрощує обробку обличчя та його характеристик шляхом використання гістограми для представлення відтінків та кольорів [92].

DCT (Discrete Cosine Transform): Використовуються функції DCTmod2 [93], видобуті з зображень обличчя розміром 40 на 32 пікселі. Для обчислення коефіцієнтів DCT використовується зображення 8 на 8 з горизонтальним і вертикальним перекриттям 50%. Отриманий результат - набір з 35 векторів ознак, кожен розмірністю 18. Ці вектори включають інформацію про структуру та особливості обличчя. Для порівняння використовуються сусідні зоображення, що додається до точності обчислень.

DCTb (Discrete Cosine Transform для більших зображень): Аналогічно DCT, але вхідне зображення обличчя має розмір 80 на 64 пікселі, що дозволяє отримати більше деталей. Набір містить 221 вектор ознак, кожен з розмірністю 18. Враховуючи більший розмір зображення, ці ознаки дозволяють враховувати більше аспектів обличчя, забезпечуючи більш точний аналіз.

Ці характеристики є ключовими для визначення і розпізнавання обличчя в системі, а їхня деталізація та оптимізація сприяють підвищенню точності та ефективності процесу розпізнавання.

Експертна система для аналізу мовлення базується на комплексі характеристик, які визначають та оптимізують її ефективність:

LFCC (The Linear Filter-bank Cepstral Coefficient) [94]: Ця характеристика використовує 24 лінійно розташованих фільтри на кожному кадрі коефіцієнтів Фур'є. Для кожного кадру обчислюються 16 коефіцієнтів DCT для кореляції з 24 коефіцієнтами логарифму спектра потужності, отриманими з банку лінійних фільтрів. До отриманого набору ознак додаються перші часові похідні.

PAC-MFCC (The Phase Auto-Correlation Mel Filter-bank Cepstral Coefficient) [95]: Ця характеристика використовує функції фазової автокореляції. Обчислюється 20 коефіцієнтів DCT для кореляції з 30

коефіцієнтами, отриманими з банку фільтрів за шкалою Мела. Додавання перших часових похідних збагачує набір функцій.

SSC (Spectral Subband Centroid): SSC, спочатку розроблений для розпізнавання мови [96], виявився ефективним для автентифікації диктора [97]. Віднімання середнього значення істотно поліпшує ці характеристики. Середньо-відняті SSC обчислюються з 16 коефіцієнтів. Важливий параметр, який регулює вплив центроїда, встановлено на рівні 0,7.

Ці характеристики взаємодіють для визначення особливостей мовлення та забезпечують комплексний підхід до аналізу для підвищення точності та надійності системи.

2.2.3 Базові системні класифікатори

FH, MLP (Multilayer Perceptron): Використовується нормалізоване обличчя, об'єднане з гістограмою, які є ознаками (FH). Для класифікації використовується MLP з 20 прихованими одиницями. MLP навчається на геометрично трансформованих зображеннях.

DCT, GMM (Discrete Cosine Transform, Gaussian Mixture Model): Ознаки обличчя - це DCTmod2, обчислені на зображенні розміром 40 x 32 пікселів, утворюючи 35 векторів ознак. GMM містить 64 гауссові компоненти, а модель світу навчається з використанням всіх клієнтів у навчальній вибірці [98].

DCTb, GMM (Modified DCT, GMM): Ознаки DCTmod2, розраховані на зображенні обличчя розміром 80 x 64 пікселів, утворюють послідовність з 221 вектора ознак. Відповідна GMM має 512 гауссових компонент.

DCT, MLP: Ознаки ті ж, що і в (DCT, GMM), за винятком того, що використовується MLP замість GMM, з 32 прихованими одиницями. Навчання виконується на одному великому векторі ознак, отриманому конкатенацією 35 векторів ознак.

DCTb, MLP: Ознаки аналогічні (DCTb, GMM), за винятком використання MLP із 128 прихованими одиницями. MLP навчається на векторі ознак з розмірністю 221 x 18.

LFCC-GMM: Ознаками (LFCC) є лінійний фільтр-банк цепстральних коефіцієнтів, витягнутих з мовних даних бази даних XM2VTS. Класифікатор (GMM) використовує модель з 200 гаусівськими компонентами, де мінімальна відносна дисперсія для кожного гауса становить 0,5, а вага адаптації MAP - 0,1. Це широко визнана та ефективна модель, яка показує високу продуктивність в різноманітних умовах [99].

PAC-GMM: Ознаками (PAC) є використання функції фазової автокореляції цепстрального коефіцієнта, аналогічно до конфігурації LFCC. Класифікатор (GMM) використовує ту ж конфігурацію GMM, що і в LFCC. Варто зауважити, що наявність 200-300 гаусівських компонент призводить до лише 1% різниці у NTER, демонструючи високу стійкість до шумових умов.

SSC-GMM: Ознаками (SSC) є використання спектрального підсмугового центроїда, аналогічно до попередніх конфігурацій. Класифікатор (GMM) використовує ту саму конфігурацію GMM, що і в LFCC. Ця система демонструє найвищу продуктивність в умовах помірного шуму (від 18 до 12 дБ), що було успішно перевірено в завданні виявлення одного динаміка за стандартом NIST2001.

Ці варіанти демонструють різноманітні комбінації ознак та класифікаторів, що дозволяють системі пристосовуватися до різних завдань біометричної ідентифікації та підтвердження, забезпечуючи оптимальний баланс між точністю та обчислювальною ефективністю.

2.3 Приклади мультимодальних систем розпізнавання особи

Дослідники, такі як К. Чибелуші, професор когнітивних цифрових медіа-обчислень, та його співавтори Ф. Дераві, професор інформаційної інженерії, та Д. Мейсон, доктор філософії в галузі управління та цифрової обробки сигналів, представили новаторську систему аудіовізуальної біометрії “Voice and facial

image integration for speaker recognition”, що використовує як акустичну, так і статичну візуальну інформацію, включаючи зображення облич. Вони використовували комплексну базу даних, яка складалася з аудіозаписів та фотографій облич десяти дикторів. Зображення були зафіксовані при різних орієнтаціях голови, різних масштабах та положеннях суб'єкта.

У ході свого дослідження вони використовували метод зваженого підсумовування для об'єднання акустичної та візуальної інформації. Результати їх системи біометричної ідентифікації вражаючі: EER склав 3,4%, 3,0% і 1,5% для випадків, коли використовувалася лише мовна інформація, лише візуальна інформація або обидві інформаційні ресурси відповідно. Це свідчить про високу точність та ефективність їхнього методу в умовах різної доступності інформації та різноманітних сценаріях застосування.

Дослідники Р. Брунеллі та Д. Фалавінья з Інституту науково-технологічних досліджень розробили вражаючу систему ідентифікації диктора “Person identification using multiple cues”, яка відрізняється тим, що вона не використовує текстової інформації та комбінує лише аудіо- та візуальні дані. Вони використовували розширену базу даних AV, яка включала в себе аудіозаписи та фотографії облич 89 спікерів.

У підході, що запропонували дослідники, використовувалося п'ять класифікаторів, з яких два були призначені для обробки акустичних ознак, а три - для візуальних. Акустичні класифікатори працювали з двома різними наборами акустичних ознак, що були отримані на основі короточасного спектрального аналізу мовного сигналу. Їхня система ідентифікації дикторів, яка взаємодіяла тільки з аудіосигналами, базувалася на використанні методу векторного квантування (VQ).

Візуальні класифікатори відповідали візуальним класифікаційним ознакам, витягнутим з трьох різних областей обличчя: очей, носа і рота. Індивідуальні класифікаційні оцінки, отримані з аудіо- та візуальних аспектів, об'єднувалися з використанням методу зваженого добутку. У результаті цього інтегрованого підходу вдалося досягти рівня ідентифікації високого рівня -

98%. Це значущий успіх у порівнянні з продуктивністю систем, які використовують тільки аудіо- чи візуальну інформацію.

Дослідник Бен-Якуб з Інституту перцептивного штучного інтелекту Далле Молле та його команда провели комплексне дослідження, створивши як текстозалежні, так і текстонезалежні системи верифікації аудіо- та відеодикторів на основі бази даних XM2VTS. У своїй роботі “Fusion of face and speech data for person identity verification” вони використовували акустичну та візуальну інформацію з фронтальної частини обличчя, а для отримання оцінок відповідності обличчя використовували еластичне зіставлення графів.

Щодо результатів, дослідники визначили, що методи злиття графіків, такі як зважене підсумовування, байєсівський класифікатор, SVM, конкатенація і модифікований байєсівський посткласифікатор, виявилися ефективними в умовах як шуму, так і чистого звуку. Це свідчить про успішність цих методів у забезпеченні стійкості та точності в умовах різного роду впливів.

Особливу увагу варто звернути на те, що вони докладно проаналізували і порівняли кілька методів злиття графіків, розглядаючи як неадаптивні, так і адаптивні підходи. При цьому вони враховували, як розподіли даних можуть змінюватися в умовах шуму, при цьому не намагаючись прямо визначити тип шуму, що присутній в тестових ознаках.

Дослідники К. Сандерсон, керівник проекту Data61/CSIRO, і К. Палівал, член Акустичного товариства Індії, фокусувалися на розробці системи “Identity verification using speech and face information”, яка використовує інформацію про мову та обличчя для незалежної від тексту верифікації особи. Для аналізу аудіосигналів, вони використовували векторну квантизацію, що є методом зменшення розмірності векторів ознак і забезпечує ефективну репрезентацію аудіо-інформації.

У системі дослідників використовувалася інформація, витягнута з трьох ключових областей обличчя: очей, носа і рота. Зображення обличчя піддавалися аналізу за допомогою методу головного компоненту (PCA), що дозволяє виявляти ключові особливості та визначати головні напрямки варіації в даних.

Для акустичної інформації використовувалися ознаки, такі як коефіцієнти MFCC та їхні дельти, а також максимальні значення автокореляції, які містять інформацію про висоту тону та голос.

Застосування детектора голосової активності (VAD) було важливим етапом для видалення тих векторів ознак, які представляли тишу або фоновий шум. Потім використовувався класифікатор змішаних гауссів (GMM) для аналізу аудіосигналів та виділення мовних ознак.

Щодо ефективності, їхня система проявила високий рівень продуктивності в умовах помірно зашумлених умов. Результати їх дослідження підкреслили успішність підходу, де комбінована інформація з аудіо та візуальних джерел дозволяє досягти точної та стійкої верифікації особи.

Команда науковців під керівництвом Б. Хейзена спроектувала текстозалежну систему для автентифікації диктора. Ця система взяла на себе завдання використовувати аудіо- та візуальні сигнали низької якості, отримані за допомогою портативного пристрою. У своїй роботі “Multi-modal face and speaker identification on a handheld device” вони застосовували алгоритм розпізнавання обличчя, базований на методі опорних векторів (SVM), який є одним з популярних методів машинного навчання [100].

Суть їхньої роботи полягала у використанні інформації про обличчя та ідентифікацію диктора для покращення точності верифікації особи. Вони досягли значного успіху, демонструючи 90% зниження ефективної співвідносної помилки (EER) у верифікації диктора. Зокрема, вони використовували інформацію про обличчя, витягнуту з 14 компонентів обличчя, та використовували SVM для класифікації та розпізнавання основних рис.

Важливим етапом в роботі науковців було зниження розмірності вхідних даних, що було досягнуто шляхом відбору та нормалізації певних рис обличчя. Це дозволило покращити якість вхідних даних для класифікації та зменшити вплив низької якості аудіо- та візуальних сигналів на результати системи. Такий підхід виявився ефективним і призвів до вражаючих результатів у сфері

автентифікації диктора, особливо при використанні комбінації інформації про обличчя та ідентифікацію диктора.

Ускладненість злиття на рівні прийняття рішень виникає через обмежену доступність інформації. Отже, зазвичай вибір виявляється на користь злиття на рівні результатів порівняння, оскільки він є більш доступним і дозволяє об'єднувати результати, отримані з різних модальностей [101].

Термін "мультимодальна біометрична система" вперше запропонований А. Россом, з відділу комп'ютерних наук та електротехніки, та іншими [102], став предметом активного дослідження у зв'язку з питанням про те, наскільки мультимодальність може вдосконалити продуктивність біометричних систем. Вчені вважали, що комбінування різних біометричних ознак може сприяти покращенню ефективності системи [103].

Згодом були представлені різні рівні злиття, де роботи "Multimodal Biometric Systems - Study to Improve Accuracy and Performance" [104], "A robust person authentication system based on score level fusion of left and right irises and retinal features" [105], "Combining face and iris biometrics for identity verification" [106] та "A principled approach to score level fusion in multimodal biometric systems" [107] вивчають інтеграцію на початку та в кінці біометричної системи.

Існує ряд підходів до злиття на рівні ознак і рішень. Наприклад, Юньхон Ван, Т. Тан та А. Джайн пропонували об'єднання обличчя та райдужної оболонки ока на рівні ознак. Злиття на рівні балів було введено С. Дассом з університету Геріот-Ватта та іншими науковцями для об'єднання мультимодальних біометричних ознак, зокрема, відбитків пальців. Цей метод був подальше вдосконалений та використаний в різних дослідженнях, зокрема у роботах В. Шайпера та інших "Robust fusion: Extreme value theory for recognition score normalization" [108].

Нещодавно деякі дослідження вивчали об'єднання райдужної оболонки ока та відбитків пальців [109]. Ці дослідження базуються на злитті на рівні ознак та рішень. Наприклад, А. Джагадісан та його команда з кафедри електротехніки Технологічного коледжу Сона [110] розробили мультимодальну систему злиття,

що комбінує відбитки пальців та райдужну оболонку ока на рівні ознак. Система показала підвищену точність порівняно з використанням одного типу біометричної модальності.

У 2011 році Д. Баша з Інженерно-технологічного коледжу VLB Janakiammal та командою [111] запропонували новий підхід для мультимодальної системи, заснованої на методі регресії, який виявився швидшим і високоефективним для отримання високих рейтингів ідентифікації. Однак, в дослідженні "Multimodal biometric system fusion using fingerprint and iris with fuzzy logic" М. Абдолахі та інших науковців [112], де використовувалася нечітка логіка та зважений код для об'єднання райдужної оболонки ока та відбитків пальців, був виявлений високий рівень розпізнавання (98%), але також високий рівень помилок (2%), що вимагає подальших вдосконалень.

Деякі дослідження використовують ієрархічний підхід "від грубого до тонкого" для мультимодальних систем. Наприклад, Чжу та Чжан [113] використовують геометрію пальців, відбитки долонь та особливості відбитків кісточок для створення нової мультимодальної біометричної інформаційно-пошукової системи. Ш. Горпаде та ін. [114] пропонують метод, що використовує райдужну оболонку ока, відбитки пальців та обличчя для оцінки якості зображень та диференціації легітимних зразків від зразків-самозванців.

У дослідженні, представленому в "Two-stage plant species recognition by local mean clustering and Weighted sparse representation classification" [115], розроблено двоетапний метод навчання класифікації для розпізнавання видів рослин з використанням локальної схожості. Однак ця система страждає від високої обчислювальної складності.

С. Бакші та ін. [116] представили систему періокулярної автентифікації, яка використовує вилучення та зіставлення ознак для швидкої мобільної біометричної автентифікації. А. Адаму у своїй роботі "Attendance management system using fingerprint and iris biometric" [117] представив систему управління відвідуванням, яка використовує біометричні методи відбитків пальців та райдужної оболонки ока для запису, моніторингу та управління відвідуванням

студентів, що складається з інтерфейсу користувача, бази даних та сканера біометричних ознак, встановленого на вході до лекційної аудиторії.

Висновки до розділу 2

Встановлено, що біометричні системи, хоча і високоефективні в ідентифікації осіб, стикаються з визначеними вразливостями. Аналіз показав, що деякі із цих вразливостей включають можливість використання підроблених біометричних даних, атаки на апаратне забезпечення та сценарії атак із використанням фальсифікації обличчя. З метою підвищення безпеки були розглянуті технічні та програмні рішення як важливий компонент системи захисту від вразливостей.

Аналіз мультимодальних біометричних систем показав, що поєднання різних біометричних характеристик сприяє створенню ефективної та надійної системи ідентифікації осіб. Розглянуті підходи до злиття біометричних даних на рівні ознак і рішень, а також вказано на переваги використання мультимодальних систем у забезпеченні високого рівня точності ідентифікації, що дозволяє збільшити витримку до вразливостей та підвищити загальну ефективність систем.

У результаті дослідження представлені конкретні приклади застосування та реалізації мультимодальних біометричних систем, які включають порівняння та оцінку підходів до злиття на рівні ознак і рішень, інтеграцію відбитків пальців та райдужної оболонки ока, а також використання ієрархічних підходів для комбінування геометрії пальців, відбитків долонь та особливостей кісточок. Зазначено, що такі системи не лише забезпечують надійність ідентифікації, але й виявляють високий рівень стійкості до атак і вразливостей, що може бути критично важливим у сучасних умовах безпеки та конфіденційності.

РОЗДІЛ 3

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ ДОСТУПОМ

3.1 Складові біометричних систем контролю і управління доступом

Система контролю та управління доступом (СКУД) є комплексом технічних пристроїв та програм, спрямованих на ефективний контроль та регулювання доступу до об'єктів, де важлива необхідність управління фізичним доступом (наприклад, в офісах, лікарнях, державних установах, на підприємствах, стоянках автотранспорту, приватних територіях та інших об'єктах) [118].

Система СКУД надає можливість вибрати оптимальну схему ідентифікації, враховуючи вимоги до безпеки та виділений бюджет. Це може бути як комплексне рішення, так і окремі точкові системи, призначені для обмеження доступу до конкретних приміщень чи ресурсів. Зокрема, пристрої контролю можуть бути інтегровані у внутрішні мережі, такі як опалювальна, протипожежна, охоронна, для забезпечення економії енергоресурсів.

Кожна система СКУД характеризується високим рівнем безпеки та надійності, що залежить від використаного обладнання та його конфігурації.

Біометричні системи контролю доступу дозволяють ефективно управляти доступом, використовуючи ідентифікацію по відбитку пальця, сітківці ока, райдужці ока, формі долоні та обличчя. Ці пристрої відзначаються відсутністю збоїв та практичною неможливістю їх обману. Це забезпечує вищий рівень безпеки порівняно з традиційними системами контролю за допомогою карток, оскільки біометричні дані набагато важче підробити. Основні переваги цієї технології включають миттєву перевірку особистості та зберігання журналу подій на мережевому контролері. Недоліками можуть бути високі витрати та невизначеність щодо можливості видавати тимчасові перепустки.

Біометричні системи контролю доступу дозволяють вести облік робочого часу, записуючи інформацію в таблиць робочого часу про час та графік робочого дня, що дає можливість відслідковувати рухи кожного працівника через пункт пропуску та ведення деталізованого обліку.

Біометричні складові СКУД показані на рис. 3.1.

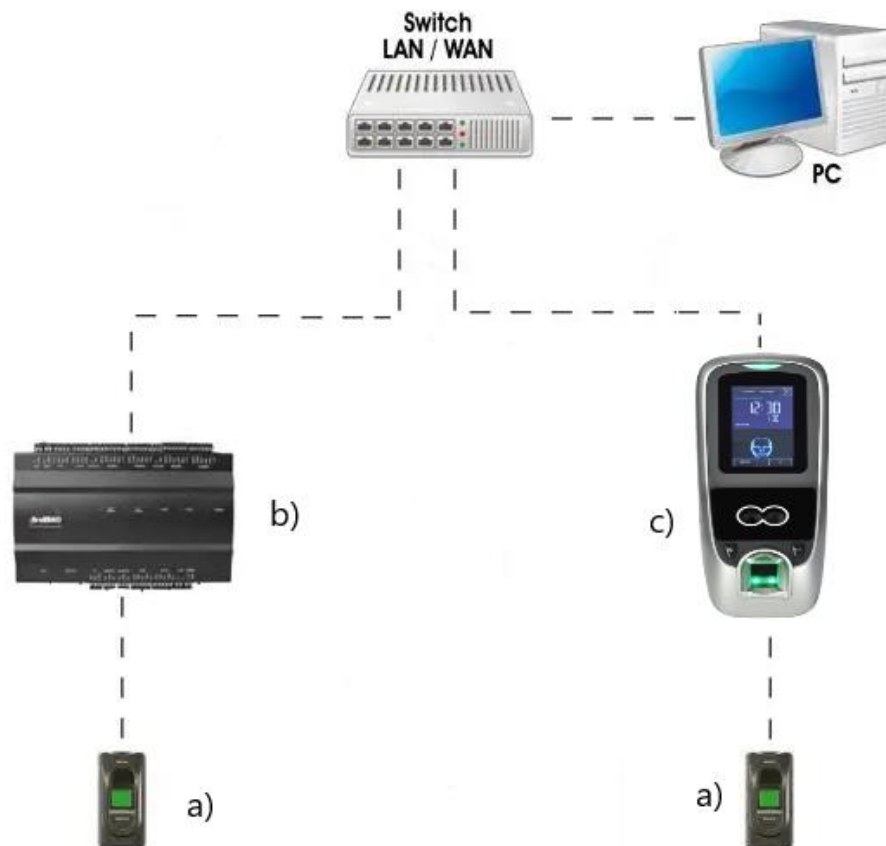


Рис. 3.1. Біометричні складові СКУД: а) Біометричний зчитувач, б) Біометричний контролер, с) Біометричний термінал

3.1.1 Біометричні зчитувачі

Біометричні зчитувачі представляють собою спеціальні пристрої, призначені для розпізнавання та ідентифікації особи на основі фізіологічних особливостей її організму [119]. Розрізняють три основних типи біометричних зчитувачів, які використовуються в системах контролю й управління доступом:

Біометричні зчитувачі без внутрішнього контролеру: такі пристрої можуть бути інтегровані в існуючі системи контролю доступу. Вони виконують

лише функцію зчитування біометричних даних, після чого вся обробка ідентифікації відбувається на підключеному контролері.

Біометричні зчитувачі з пам'яттю на події: схожі на попередній тип, але зберігають інформацію про події проходження власною пам'яттю. Це надає додаткову гнучкість і можливість аналізу історії проходжень безпосередньо на самому пристрої.

Керовані біометричні зчитувачі: використовуються для створення мережових точок проходу з високим рівнем безпеки. Вони можуть слугувати як односторонні, так і двосторонні точки доступу, залежно від підключення біометричного терміналу чи контролера.

Один із найпоширеніших методів біометричної ідентифікації – розпізнавання за відбитком пальця. Кожна особа має унікальні папілярні візерунки, які сканер відбитків пальців реєструє і перетворює в цифровий код для подальшої ідентифікації.

Технологія розпізнавання за сітківкою ока використовує зображення кровоносних судин в очах, що вимагає освітлення та сканування спеціальною камерою. Розпізнавання за райдужною оболонкою ока ґрунтується на особливостях саме райдужки, що також вимагає спеціального сканера та обробки отриманого коду.

Біометричний зчитувач за формою долоні отримує тривимірний знімок руки та трансформує його в код для подальшої ідентифікації. За допомогою розпізнавання обличчя можна створювати дво- або тривимірні образи для подальшої ідентифікації.

Засоби біометричного сканування відбитків пальців можна класифікувати за технологією на: ультразвукові; напівпровідникові; оптичні.

Зокрема, оптичні зчитувачі, які використовують світловий промінь для сканування, стали найбільш поширеними на ринку систем охорони та безпеки.

3.1.2 Біометричні контролери

Біометричний контролер виступає як ключовий елемент в системі управління та контролю доступу, співпрацюючи з біометричним зчитувачем[120]. Контролер відповідає за збереження та обробку архіву ідентифікаторів, наприклад відскановані відбитки пальців, і проводить порівняння отриманих ідентифікаторів з наявною базою даних, вирішуючи питання щодо надання чи обмеження доступу.

Біометричні контролери поділяються на два основні типи:

Автономні біометричні контролери обробляють інформацію, отриману від зчитувачів, і самостійно дозволяють чи забороняють доступ. Ці контролери можуть зберігати необхідні зразки ідентифікаторів у пам'яті для подальшого порівняння.

Мережеві біометричні контролери виконують такі ж завдання, як і автономні, проте вони мають можливість приєднання до мережі. Це дозволяє мережевим біометричним контролерам використовувати базу ідентифікаторів не лише з власної пам'яті, але й з інших джерел.

Для організації розподілених мережесистем контролю та управління доступом, біометричні контролери підтримують інтерфейси RS485 та Ethernet. Використання Ethernet виявляється особливо зручним, оскільки пристрої контролю доступу інтегруються в мережеву IP інфраструктуру, що спрощує адміністрування мережесистем контролю доступу. Це надає можливість мережевому адміністратору ефективно супроводжувати рішення системи контролю та управління доступом без додаткового залучення персоналу для обслуговування.

3.1.3 Біометричні термінали

Біометричний термінал є інноваційним пристроєм, розташованим на вході до об'єкта чи території, спрямованим на забезпечення контролю доступу, обліку робочого часу, підвищення рівня безпеки та ефективного управління

електронними замками та турнікетами [121]. Наведені нижче особливості визначають унікальні можливості даних технологічних пристроїв.

Мережева та автономна робота: Біометричні термінали можуть працювати в мережевому режимі або в автономному, це надає гнучкість у використанні та інтеграції з різними системами безпеки.

Цифрова клавіатура та функціональний екран: Біометричні термінали можуть бути оснащені цифровою клавіатурою для введення коду, виклику підтримки та переходу до меню налаштувань. Також деякі з них мають екран та функцію розпізнавання геометрії обличчя та фотографування осіб.

Багаторівнева ідентифікація: Термінали часто включають в себе сканер відбитка пальця та можливість зчитування безконтактних карт (RFID), що забезпечує багаторівневий підхід до ідентифікації особи.

Антивандальний корпус та оповіщення: Антивандальний корпус і система оповіщення, якими додатково обладнуються термінали, після неправомірних спроб доступу гарантують захист від зовнішніх механічних впливів і забезпечують безпеку об'єкта.

Біометричні термінали обліку робочого часу базуються на ідентифікації за біологічними та анатомічними характеристиками людини. Інтеграція терміналів реєстрації дозволяє підвищити безпеку та оптимізувати процес обліку робочого часу, надаючи можливість фіксації часу приходу та виходу співробітників.

Біометричні термінали можуть бути розміщені у вигляді настінних, напільних чи настільних установок. Вони ефективні для використання на об'єктах з високим рівнем вимог до безпеки, таких як військові, промислові, медичні та фінансові установи, офісні приміщення та бізнес-центри.

3.2 Огляд технічних засобів біометричних СКУД бренду ZKTeco

ZKTECO CO, LTD. (ZKTeco) - це всесвітньо відома компанія, яка спеціалізується на передових технологіях біометричного розпізнавання, а також надає продукти і рішення для розумного управління входом, розумної автентифікації особистості та розумного офісу [122]. ZKTeco пропонує послуги на всіх рівнях для державних служб, підприємств і приватних користувачів.

ZKTeco є перевіреним постачальником алгоритмів біометричної верифікації, сенсорів і програмної платформи, який володіє патентами на методи розпізнавання відбитків пальців, райдужної оболонки ока, обличчя, вен і долоні тощо. Компанія володіє патентами на методи комп'ютерного зору, включаючи розпізнавання обличчя, ідентифікацію поведінки, ідентифікацію рентгенівських об'єктів та відеоструктуру, що робить ZKTeco одним з підприємств у галузі, яке володіє порівняно великою кількістю патентів. Перелік винаходів компанії є досить широким: від основних технічних дозволів на фізичні та поведінкові особливості, включаючи відбитки пальців, райдужну оболонку ока, обличчя та вени, до програмного забезпечення ZKBioDeSee, оснащеного гібридною біометричною верифікацією та комп'ютерним зором, а також гібридною біометричною верифікацією та аутентифікацією особистості O2O смарт-терміналів і рішень, що базуються на інтелектуальних додатках для верифікації й аутентифікації особи.

3.2.1 Біометричні зчитувачі ZkTeco FR1500

Біометричний зчитувач ZKTeco FR1500 (Рис. 3.2) представляє сучасне технічне рішення, спрямоване на вдосконалення систем контролю доступу та забезпечення високого рівня безпеки. Завдяки своїй продуктивності та надійності, цей зчитувач здатний забезпечити ефективну ідентифікацію осіб та забезпечити контроль над доступом в об'єкти.

ZKTeco FR1500 використовує передовий сенсор SilkID для точного зчитування відбитків пальців. Версія алгоритму ZK Finger v10.0 дозволяє ефективно обробляти та аналізувати отримані біометричні дані, забезпечуючи надійну ідентифікацію користувачів. Інтерфейс RS485 забезпечує швидку та стабільну передачу зображень відбитків пальців для обробки інформації на контролерах серії inBio або біометричних терміналах.



Рис. 3.2. Біометричний зчитувач ZKTeco FR1500

Однією з ключових особливостей зчитувача є можливість аутентифікації користувачів не лише за допомогою відбитків пальців, а й за допомогою безконтактних карток Em-Marine. Ця універсальність дозволяє використовувати різні методи ідентифікації, що забезпечує зручність та гнучкість в експлуатації.

Біометричний зчитувач ZKTeco FR1500 відзначається високою стійкістю до погодних умов, дозволяючи встановлювати його як у приміщенні, так і на вулиці. Захист від вологи та пилу на рівні IP65 гарантує надійну роботу зчитувача навіть в екстремальних умовах. Додатково, забезпечено звукову індикацію за допомогою бузера, що сприяє ефективному використанню зчитувача.

3.2.2 Біометричні контролери ZkTeco inBio160/260/460

Контролер InBio260, вироблений компанією ZKTeco (Рис. 3.3), призначений для ефективного управління доступом і визначення особистості в

об'єктах зі збереженням високого рівня безпеки. Зазначений контролер розроблений для управління доступом до двох дверей і підтримує як одно-, так і двосторонній контроль. Він може легко інтегрувати 4 зовнішні біометричні зчитувачі ZKTeco inBio або 4 зчитувачі Wiegand.



Рис. 3.3. Біометричний контролер ZKTeco InBio260

Основні функціональні особливості контролера InBio260 включають в себе використання високошвидкісного 32-розрядного процесора з тактовою частотою 400 МГц, 32 МБ оперативної пам'яті та 256 МБ Flash-пам'яті. Забезпечується висока ефективність завдяки вбудованій операційній системі LINUX.

Цей контролер може зберігати і обробляти інформацію про 30 000 RFID карт, 3000 шаблонів відбитків пальців та 100 000 записів у журналі подій. Забезпечена підтримка різних форматів карт Wiegand і клавіатурного пароля для збільшення гнучкості в системі безпеки.

Використання технологій зв'язку, таких як Ethernet і шина RS485, робить контролер InBio260 високопродуктивним у веденні обліку та контролі за доступом. Він має вбудований апаратний сторожовий таймер, що запобігає можливим збоям, а також захист від перевантажень для адаптера живлення та зовнішніх зчитувачів.

Технічні характеристики контролера включають можливість підключення 8 зчитувачів (4 RS485 зчитувачі та 4 26-бітних Wiegand зчитувачі), різні типи зчитувачів, 6 входів та 4 виходи, а також підтримку зв'язку через TCP/IP та RS485.

3.2.3 Біометричні термінали ZKTeco WL30

Біометричний термінал ZKTeco WL30 розроблений для ефективної організації систем обліку робочого часу, представляючи інноваційні можливості та високотехнологічні характеристики. Завдяки своїм компактним розмірам і стильному дизайну, цей термінал є ідеальним рішенням для точного відслідковування робочого часу працівників, використовуючи біометричні дані, такі як відбиток пальця та індивідуальний код.



Рис. 3.4. Біометричний термінал ZKTeco WL30

В основі терміналу лежить високоточний сканер відбитків пальців BioID, що забезпечує надійне зчитування навіть мокрих відбитків пальців за умови яскравого освітлення. Це робить процес реєстрації простим та ефективним. Система також дозволяє працівникам самостійно фіксувати час приходу та відходу, забезпечуючи автономність та легкість в користуванні.

Наявність вбудованого Wi-Fi-модулю робить термінал ZKTeco WL30 особливо зручним, оскільки не вимагає прокладання додаткових комунікаційних ліній. Додатковим плюсом є вбудований дисплей та інтуїтивно зрозумілий інтерфейс, які спрощують налаштування та додавання нових користувачів, навіть для осіб без попередньої підготовки. Зручність доступу до звітів, як з комп'ютера, так і з мобільного додатку, робить процес моніторингу ще більш гнучким і доступним.

Характеристики терміналу вражають своєю функціональністю: можливість реєстрації 1000 відбитків, зберігання 50 000 записів, використання передового сенсора BioID та версії алгоритму ZK Finger v10.0. Забезпеченість

різноманітними інтерфейсами зв'язку, такими як Wi-Fi та USB, підкреслює готовність термінала впроваджуватися в різноманітні корпоративні інфраструктури.

3.2.4 Мультибіометричні термінали ZKTeco FV18

Мультибіометричний термінал ZKTeco FV18 (Рис. 3.5) використовується для імплементації СКУД на основі біометричних даних, таких як рисунок вен та відбитки пальців. Оснащений апаратною платформою, що базується на платі ZMM220 із процесором 1.2 ГГц, цей термінал вирізняється гнучкістю в побудові систем контролю доступу. Він підтримує як автономне встановлення, так і комунікацію з будь-якими сторонніми контролерами керування доступом, що використовують стандартний інтерфейс Wiegand. Забезпечує зв'язок з комп'ютером або сервером бази даних через USB-диск, Ethernet та USB інтерфейси, інтегруючись легко в системи СКУД.



Рис. 3.5. Мультибіометричний термінал ZKTeco FV18

Термінал ZKTeco FV18 дозволяє автоматизувати облік робочого часу працівників, використовуючи для ідентифікації рисунок вен, відбиток пальця, код або безконтактну картку (за вибором користувача). Ця система ідентифікації та верифікації гарантує уникнення випадкових або навмисних випадків саботажу та точний облік часу приходу/виходу працівників.

Додатково, термінал оснащений світлозвуковим сповіщенням для нормальної роботи, сигналом тривоги при спробі демонтажу, охоронним сповіщенням після повторних спроб несанкціонованого доступу та функцією "палець під примусом", що дозволяє доступ лише за умови одночасного відправлення сигналу тривоги.

Характеристики терміналу включають кольоровий 2.4" TFT дисплей, пам'ять для 1000 шаблонів відбитка пальця та 1000 шаблонів вен, а також можливість зберігання 5000 карток Em-marin і журналу подій на 100000 записів. Він оснащений сенсором відбитка вен ZK Finger Vein, алгоритмами розпізнавання ZKFinger VX10.0 і ZKFingerVein VX3.0. Інтерфейси включають TCP/IP, USB, Wiegand, а також підтримку додаткових функцій, таких як DST, Record Query та Anti-passback. Програмне забезпечення включає SDK та ZKAccess 3.5.

3.2.5 Мультибіометричні термінали ZKTeco Multibio700

Мультимодальний біометричний термінал Multibio700 (Рис. 3.6) забезпечує широкий спектр застосувань у системах контролю та обліку робочого часу для забезпечення безпечного та ефективного доступу до приміщень. Цей термінал володіє здатністю ідентифікації за допомогою обличчя, відбитка пальця, безконтактної картки та коду, що робить його надзвичайно універсальним та адаптованим до різних потреб бізнес-середовищ.



Рис. 3.6. Мультибіометричний термінал ZKTeco Multibio700

Пристрій працює на основі зчитування відносної позиції, розміру і форми ключових елементів обличчя, таких як очі, ніс, скули, щелепа, для формування біометричного шаблону. Цей шаблон використовується для подальшого порівняння та ідентифікації особи, забезпечуючи точність та швидкість процесу в межах 1 секунди.

Умови недостатнього освітлення не є перешкодою завдяки інфрачервоному підсвічуванню, яке забезпечує успішну ідентифікацію навіть при обмеженому освітленні. Зазначені характеристики пристрою також включають велику кількість збережених шаблонів обличчя (1500), відбитків пальців (2000) та безконтактних карт (10000), що робить його ідеальним для великих організацій.

Щодо додаткових можливостей, Multibio700 включає інфрачервону камеру високої роздільної здатності, сенсорний дисплей розміром 3 дюйми, а також підтримку різних інтерфейсів зв'язку, включаючи RS485, TCP/IP та USB-host. Зокрема, вбудований RFID читач (125kHz RFID Em-Marine) додає ще один рівень безпеки та комфорту для користувачів.

Такий біометричний термінал також володіє рядом функцій контролю доступу, таких як електронний замок, геркон, кнопка виходу та сирена. Зазначені функції дозволяють налаштовувати 50 тимчасових зон, 5 груп доступу й 10 комбінацій розблокування, забезпечуючи високий рівень адаптації до конкретних потреб користувача.

Застосування технології ZK Face v7.0 і ZK Finger v10.0 в роботі пристрою забезпечує високий рівень ефективності та безпеки в системах контролю та обліку робочого часу.

3.3 Технологія розпізнавання обличчя Face ID

На сьогоднішній день, найбільш широко використовуваним методом перевірки особистості людини є порівняння рис обличчя з фотографіями у документах, таких як паспорт чи водійські права, для встановлення ідентичності особи. У сфері біометричної авторизації вже успішно використовується Face ID - сервіс для розпізнавання та порівняння обличчя, надійний додатковий фактор безпеки, особливо в роботі з клієнтами фінансових установ та інших галузей [123].

Важливо відзначити різницю між двома підходами: розпізнаванням обличчя (Facial Recognition) та порівнянням обличчя (Face Comparison), хоча обидва використовують одну і ту ж технологію. Розпізнавання обличчя передбачає пошук збігів із зображенням у великій базі даних і застосовується в правоохоронних органах, системах безпеки, банківській сфері та споживчому секторі. Програми для порівняння обличчя реалізують порівняння двох фотографій однієї людини.

Біометричні системи розпізнавання обличчя ґрунтуються на принципі побудови і порівняння математичних моделей особи, що дозволяє ідентифікувати або верифікувати особистість з високою точністю. Ці системи формують гіпотезу щодо того, чи збігається особа на одній фотографії з особою на іншій, не залежно від виразу обличчя та інших ознак, таких як вік, зачіска, аксесуари тощо.

Вагомою перевагою є те, що камери, які використовуються для Face ID, здатні захопити зображення на відстані, що ідеально підходить для створення систем моніторингу та прихованої ідентифікації, що робить безконтактну біометрію ще більш привабливою в контексті використання Face ID в корпоративному оточенні.

3.3.1 Сфери застосування Face ID

Технології розпізнавання обличчя використовують у багатьох сферах, серед яких банківсько-фінансова, комерційна, логістика, митний контроль та інші (Рис. 3.7)

У контексті використання системи Face ID для біометричної авторизації в **банківському і фінансовому секторах** можна визначити кілька ключових аспектів:

Забезпечення дотримання принципу "Знай свого клієнта" (Know Your Client, KYC) у сфері протидії міжнародним фінансовим злочинам, відмиванню грошей та незаконним корупційним схемам визначається шляхом реалізації процедур KYC, які включають в себе перевірку офіційних документів, ідентифікацію особи та біометричну верифікацію. Ці процедури спрямовані на перевірку й підтвердження того, що клієнти фінансових установ є тими, ким вони себе називають.

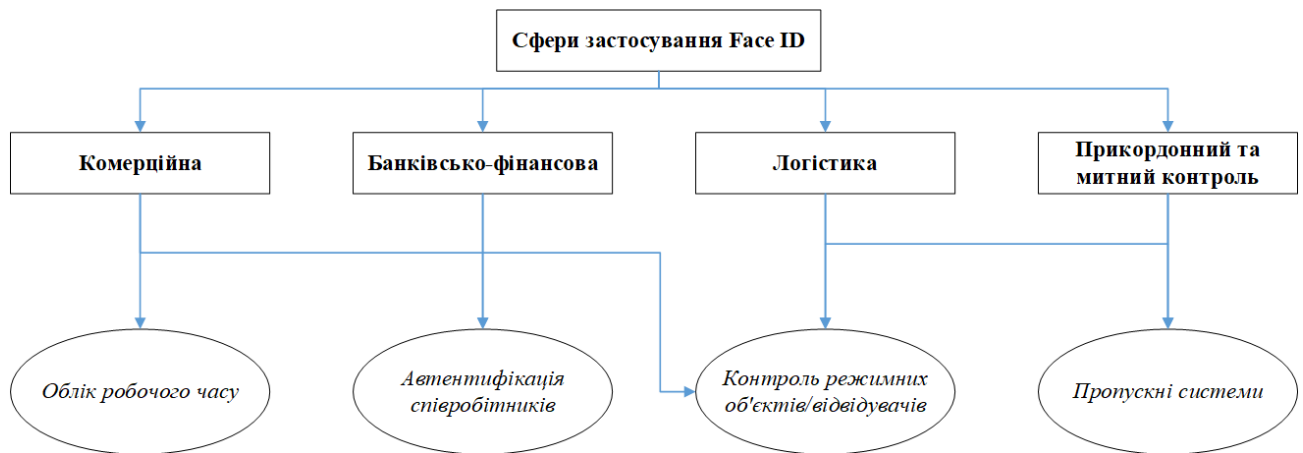


Рис. 3.7. Сфери застосування Face ID

Впровадження *біометричних банкоматів*, які замість традиційного PIN-коду використовують розпізнавання обличчя, представляє інноваційний метод забезпечення безпеки та зручності для клієнтів. Під час використання таких банкоматів, користувач вставляє свою банківську картку, і вбудована камера автоматично фотографує його обличчя. Для завершення верифікації, власник картки підтверджує свою особу, введенням пароля (який надсилається на

мобільний телефон). Цей метод не лише забезпечує високий рівень безпеки, але й покликаний полегшити процес використання банкоматів для клієнтів.

Використання системи Face ID у *фінансових установах* для порівняння фотографій клієнтів з різними базами даних визначається необхідністю боротьби з шахрайством і мінімізації ризиків. Цей метод дозволяє ефективно ідентифікувати клієнтів шляхом порівняння їхніх фотографій із заздалегідь встановленими базами даних, що сприяє уникненню несанкціонованого доступу й підвищенню рівня безпеки.

Крім того, використання Face ID в банківському та фінансовому секторах дозволяє додатково захищати систему від внутрішніх загроз шляхом ідентифікації та виключення нечесних працівників, які можуть бути втягнуті в корупційні схеми.

Отже, використання системи Face ID у фінансових установах визначається не лише потребою забезпечення безпеки та ефективності процесів, але й необхідністю відповідати сучасним стандартам індустрії у сфері ідентифікації та авторизації.

Впровадження системи розпізнавання обличчя у **комерційних установах** має стратегічне значення для вирішення ряду важливих завдань:

Застосування технології розпізнавання обличчя у *торговельних точках* може ефективно запобігати магазинним крадіжкам та організований злочинності. Система дозволяє ідентифікувати вже відомих злодіїв або потенційно агресивних відвідувачів на вході в магазин, надаючи можливість персоналу та службі безпеки реагувати в реальному часі, тим самим забезпечуючи високий рівень безпеки.

Інтеграція системи розпізнавання обличчя дозволяє підраховувати кількість відвідувачів та аналізувати їхні демографічні параметри, такі як стать, вік та етнічна приналежність. Це допомагає визначати *демографічний профіль цільової аудиторії* та сприяє удосконаленню стратегій продажу та обслуговування клієнтів.

Використання технологій розпізнавання обличчя дозволяє персоналізувати клієнтський досвід, синхронізувати його з іншими програмами для роздрібною торгівлі, системами лояльності та точками продажу (POS). Це підвищує рівень обслуговування покупців та сприяє їхній задоволеності від покупок.

Система розпізнавання обличчя може служити частиною процесу верифікації платежів на касах самообслуговування. У наведених прикладах, таких як магазини Amazon Go та служба FacePay24 в Україні, біометрична оплата вже успішно впроваджується, спрощуючи процес оплати та уникнення ручної верифікації.

У галузі **логістики** системи розпізнавання обличчя стають важливим інструментом для оптимізації різноманітних процесів, сприяючи вдосконаленню роботи логістичних компаній.

Наприклад, для *експрес-доставки*, вже впроваджено використання систем розпізнавання обличчя у службі доставки концерну Alibaba в Китаї. Ця інноваційна система дозволяє сканувати обличчя відправника за 1-2 секунди, замість традиційної перевірки особистого ідентифікаційного документа, що відчутно прискорює процес відправлення листів та посилок. Користувачам для використання цієї послуги потрібно заздалегідь завантажити необхідну інформацію, таку як адреса відправки та особа, що здійснює відправку, через один із додатків Alibaba.

Face ID також знаходить широке застосування для *ідентифікації водіїв* за фото та забезпечення безпеки перевезення спеціальних вантажів, наприклад, рецептурні препарати та медичне обладнання. Системи розпізнавання обличчя можуть бути використані для відстеження процесу доставки на кожному етапі, а також для підвищення безпеки вантажівок. Вони дозволяють ідентифікувати водіїв, впізнавати їх у різних сценаріях, та використовувати дані для вивчення стану та уваги водіїв під час поїздки, забезпечуючи високий рівень безпеки та уникнення можливих негараздів.

У сфері **прикордонного та митного контролю** Face ID вже інтегровані для спрощення в'їзду та виїзду міжнародних пасажирів в аеропортах. Ці системи

автоматизують паспортний контроль, дозволяючи прискорити процеси на пунктах перетину кордонів, проходженні митниці та підвищити рівень безпеки.

У сфері обслуговування та відпочинку системи ідентифікації обличчя вирішують ряд завдань, спрямованих на поліпшення ефективності та забезпечення безпеки в області авторизації. Ідентифікація обличчя, інкорпорована у систему Face ID, сприяє оптимізації процесів у таких сценаріях:

Застосування швидкої та ефективної верифікації відвідувачів на заходах різного масштабу (концерти, ігри, конференції) дозволяє уникнути утворення непотрібних черг. Система ідентифікації обличчя спрощує та прискорює процес входу для кожного відвідувача.

Завдяки системі Face ID гості готелю можуть скористатися кіосками самостійного реєстрування в готелі, замість традиційного оформлення на рецепції. Це робить процес реєстрації більш зручним та витонченим, зменшуючи час очікування і забезпечуючи більш високий рівень обслуговування.

Використання розпізнавання обличчя може замінити традиційні клубні карти та абонементи в спортивних клубах. Це не лише зробить обслуговування більш зручним для користувачів, але й підвищить рівень безпеки, оскільки виключає можливість неправомірного використання клубних карт.

Використання Face ID як системи біометричної авторизації для підвищення рівня безпеки корпоративних систем на різних етапах організаційного процесу займає ключове місце в **бізнес-процесах**.

Одним із важливих напрямків застосування є *автентифікація на робочому місці*, що визначається як ефективний метод підвищення безпеки та виключення можливості неправомірної передачі пароля третім особам. Використання технології Face ID гарантує надійну ідентифікацію працівників та запобігає можливості несанкціонованого доступу до корпоративних ресурсів.

Автентифікація співробітників, які працюють з дому, є ще однією важливою сферою застосування Face ID. Забезпечення обов'язкової умови для віддаленого доступу до внутрішньої інформації компанії, а також використання

liveness detection, яка гарантує вхід тільки уповноваженим працівникам, стає важливим елементом безпеки при організації віддаленої роботи.

Пропускні системи використовують Face ID як додатковий рівень ідентифікації. Це не тільки обмежує ризик проникнення на територію чи в будівлю за допомогою чужих або підроблених перепусток, але також забезпечує зручність для працівників, оскільки не вимагає наявності фізичного "ключа" при собі.

Контроль режимних об'єктів та відвідувачів стає більш ефективним завдяки терміналам з розпізнаванням обличчя. Внесення працівників до спеціальних списків та використання 'чорних списків' для небажаних відвідувачів дозволяє обмежити доступ лише уповноваженим особам та забезпечити високий рівень безпеки в режимі реального часу.

Окрім того, система біометричної авторизації Face ID може бути успішно використана для *обліку робочого часу*. Вона надає можливість точного фіксування часу, коли працівник починає і завершує роботу, а також синхронізації цих даних з системами обліку, що є необхідним аспектом при ефективному управлінні робочим часом та персоналом.

Отже, використання Face ID у біометричних системах авторизації працівників визначається широким спектром застосувань, що не тільки підвищують рівень безпеки, але й забезпечують ефективне та зручне управління корпоративними ресурсами та персоналом.

3.3.2 Розпізнавання живої присутності

Для ефективного захисту особистих даних та уникнення онлайн-шахрайства, важливо впроваджувати механізми анти-спуфінгу, такі як *liveness detection*, під час розпізнавання обличчя [124]. Ці механізми необхідні для забезпечення високого рівня безпеки при дистанційній аутентифікації користувачів.

Незважаючи на те, що біометричні системи ідентифікації є досить складними, вони часто піддаються різноманітним спробам атак, спрямованим

на обхід системи розпізнавання. Типові спуфінг-атаки включають в себе використання цифрових або роздрукованих фотографій з вирізаними отворами для очей, відеозаписів, діпфейків, а також виготовлення 2D та 3D-масок.

Зловмисники також можуть використовувати справжні біометричні дані жертви для обману систем авторизації. Це може бути і використання зловмисниками фотографій відомих людей, стокових знімків, або навіть власних фотографій, які, завдяки вмілому гриму або темним окулярам, можуть ускладнити розпізнавання осіб. Додатковими методами обходу може бути використання фотографій неіснуючих осіб або персонажів, щоб уникнути виявлення в "чорному списку".

Розпізнавання живої присутності (*Liveness Detection*) є важливим засобом безпеки, спрямованим на перевірку справжності фізичної присутності особи перед біометричною системою. Хоча розпізнавання обличчя є ефективним інструментом для ідентифікації осіб, воно не здатне гарантувати, що обличчя, яке представлено для авторизації, належить реальній особі.

Процес розпізнавання присутності особи охоплює аналіз взаємодії системи з реальною людиною має на меті уникнення використання підроблених ідентифікаторів, таких як фотографії обличчя, відеозаписи, маски або діпфейки.

Існує кілька підходів до розпізнавання присутності особи. Активне розпізнавання включає в себе інструкції для користувача щодо виконання конкретних дій чи жестів, таких як обертання голови або виконання певного жесту. Ця методика називається "*виклик-відповідь*" (*challenge-response*). З іншого боку, пасивне розпізнавання використовує внутрішні алгоритми обробки зображень для автоматичного визначення автентичності обличчя, не вимагаючи активної участі користувача.

Застосування біометричних методів, які поєднують різноманітні техніки розпізнавання, спрямоване на забезпечення високого рівня безпеки. Також можуть використовуватися більш складні апаратні методи, враховуючи технології 3D та інфрачервоного вимірювання, які аналізують контури, глибину, текстуру шкіри та рух для ефективного виявлення підробок. Важливо

враховувати, що використання таких технологій може вимагати високотехнологічного обладнання, включаючи обладнання на боці користувача.

Визначення справжності особи є ключовим фактором для забезпечення високої точності в системах автентифікації, особливо коли система віддаленого доступу функціонує без прямого контролю з боку користувача. Наприклад, у сфері безпеки цифрових облікових записів, використання технології *liveness detection* гарантує, що лише реальні особи можуть отримати доступ до акаунтів у режимі онлайн, вимагаючи їх фізичної присутності.

Додатковий рівень безпеки може бути досягнутий шляхом впровадження анти-спуфінгу з перевіркою на справжність особи. Це стає необхідним при багатофакторній автентифікації, де така перевірка виключає ризик недозволеного доступу за допомогою чужих облікових даних, забезпечуючи додатковий контроль і безпеку при обробці особистих інформаційних ресурсів.

У сфері онлайн-банкінгу та фінансових послуг використання технології *liveness detection* стає важливою складовою процесу "Знай свого клієнта" (KYC) під час онлайн-верифікації клієнтів. Ця технологія застосовується в електронних фінансових операціях, мобільному банкінгу, операціях з вилучення готівки в банкоматах без картки, процесі оформлення кредитів онлайн та інших фінансових послуг, забезпечуючи надійний рівень безпеки та автентифікації користувачів.

Перевірка справжності особи також дозволяє підтвердити вік клієнта для отримання доступу до конкретного контенту, що посилює *безпеку клієнта в цифровому середовищі*. Крім того, в інших випадках, коли використовується біометрична ідентифікація та автентифікація користувача, технологія *liveness detection* забезпечує надійний і ефективний спосіб підтвердження реальності особи, запобігаючи можливим атакам і зловживанням з боку користувачів.

Висновки до розділу 3

У результаті дослідження зроблено висновок, що завдяки практично цілковитій відсутності збоїв і мінімальним можливостям обману впровадження біометричних систем контролю доступу може значно покращити безпеку та зручність управління доступом. Водночас, важливо враховувати особливості кожної системи при її виборі та налаштуванні. Таким чином, біометричні технології можуть ефективно використовуватися для забезпечення безпеки об'єктів у різних галузях і допомагати вирішувати завдання контролю доступу сучасного підприємства.

З'ясовано, що ринок України активно впроваджує біометричні системи контролю доступу, зокрема бренду ZKTeco, який представляє різні моделі та технології біометричної ідентифікації. Аналіз ринку дозволив виявити переваги та недоліки різних систем, що сприятиме обґрунтованому вибору технологій відповідно до потреб і можливостей конкретної організації.

Встановлено, що біометричні системи розпізнавання обличчя, мають значний потенціал для практичного застосування в сфері контролю доступу, а також управління корпоративними ресурсами і персоналом. Так, засоби розпізнавання обличчя забезпечують автентифікацію персоналу на робочому місці та працівників, які працюють віддалено; посилення ефективності пропускних систем, в тому числі на режимних об'єктах; облік робочого часу персоналу.

ВИСНОВКИ

У результаті дослідження встановлено, що біометрія є синтезом технологічних і наукових методів автентифікації, заснованих на біологічних особливостях людини, які сьогодні широко застосовуються в галузі ІТ та безпеки. Використання унікальних фізичних і поведінкових характеристик особи забезпечує високу надійність методів ідентифікації, що перевершують традиційні методи із застосуванням паролів чи карток доступу.

Аналіз розвитку біометричних технологій показав, що на їх розвиток і розповсюдження позитивно вплинули стандартизація, розвиток апаратних засобів і зростання потужності обчислювальної техніки. Ці фактори взаємодіють для забезпечення успішного впровадження біометричних технологій і визначають їхню важливу роль у сучасних системах ідентифікації.

Біометричні технології поділяють на дві групи: біологічну й поведінкову. Біологічна біометрія, яка базується на фізіологічних і біологічних характеристиках організму (відбитки пальців, сітківка ока й обличчя), є однією з найперспективніших. Враховуючи унікальність і стійкість цих параметрів, методи біологічної біометрії не лише дозволяють ефективно вирішувати завдання ідентифікації, але й широко застосовуються у сфері безпеки і медицини.

Аналіз показав, що за останні роки значно зріс інтерес до технологій поведінкової біометрії, які базуються на ідентифікації індивідуальних особливостей, таких як манера ходьби, письма, спосіб введення тексту на клавіатурі, і забезпечують додатковий рівень безпеки.

Використання мультимодальних біометричних систем, які поєднують розпізнавання різних біометричних характеристик, сприяє підвищенню ефективності надійності й точності ідентифікації, а також дозволяє збільшити стійкість до атак і вразливостей, що може бути критично важливим у сучасних умовах безпеки та конфіденційності.

Зроблено висновок, що завдяки практично цілковитій відсутності збоїв і мінімальним можливостям обману впровадження біометричних систем може значно покращити безпеку і зручність управління доступом. Водночас, важливо враховувати особливості кожної системи при її виборі та налаштуванні. Також слід пам'ятати, що біометричні системи, хоча і є високоефективними засобами ідентифікації, стикаються з певними вразливостями, зокрема використання підроблених біометричних даних, атаки на апаратне забезпечення та сценарії атак із використанням фальсифікації обличчя.

З'ясовано, що ринок України активно впроваджує біометричні системи контролю доступу, зокрема бренду ZKTeco, який представляє різні моделі та технології біометричної ідентифікації. Аналіз ринку дозволив виявити переваги й недоліки різних систем, що сприятиме обґрунтованому вибору технологій відповідно до потреб і можливостей конкретної організації.

Дослідження засвідчило, що біометричні системи розпізнавання обличчя, мають значний потенціал для практичного застосування в сфері контролю доступу, а також управління корпоративними ресурсами і персоналом. Так, засоби розпізнавання обличчя забезпечують автентифікацію персоналу на робочих місцях і віддалено; посилення ефективності пропускних систем, в тому числі на режимних об'єктах; облік робочого часу персоналу.

СПИСОК ПОСИЛАНЬ

1. R. Alexander, Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures? A Quantitative Study, *Journal of Information Security*, 8 (2017). 166 p.
2. D.W. Sanders, S.K. Kaufman, B.B. Holmes, M.I. Diamond, Prions and protein assemblies that convey biological information in health and disease, *Neuron*, 89 (2016), pp. 433-448.
3. M.W. Khan, M. Sharif, M. Yasmin, S.L. Fernandes, A new approach of cup to disk ratio based glaucoma detection using fundus images, *Journal of Integrated Design and Process Science*, 20 (2016), pp. 77-94.
4. A. K. Singh, A. Mohan (eds.), *Handbook of Multimedia Information Security: Techniques and Applications*, Springer Nature Switzerland (2019), pp. 15-35.
5. Проценко Л. А. Актові книги як джерело до вивчення спеціальних історичних дисциплін // *Історичні джерела та їх використання*. (1964), pp. 52-63.
6. Шведова О. В. Дактилоскопичні дослідження : Навч. посіб. для студ. ВНЗ. Київ, КНТ (2010). 208 с.
7. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Київ, 2023.
8. ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT). Київ, 2019.
9. ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT). Київ, 2019.
10. ДСТУ ISO/IEC 27013:2017 Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT). Київ, 2019.

11. ДСТУ ISO/IEC 27039:2017 Інформаційні технології. Методи захисту. Вибірання, розгортання та експлуатування систем виявлення та запобігання вторгненням (СВЗВ) (ISO/IEC 27039:2015, IDT). Київ, 2019.
12. Загальний регламент про захист даних (GDPR). URL: <https://gdpr-text.com/uk/read/article-5/>.
13. Велика китайська кіберстіна. URL: https://uz.ligazakon.ua/ua/magazine_article/EA015310.
14. R.P. Wildes. Iris recognition: an emerging biometric technology, *Proceedings of the IEEE*, 85 (1997), pp. 1348-1363.
15. M. Sharif, M.A. Ali, M. Raza, S. Mohsin, Face recognition using edge information and DCT, *Sindh University Research Journal-SURJ (Science Series)*, (2015), 43 p.
16. J.H. Shah, M. Sharif, M. Raza, A. Azeem, A Survey: Linear and Nonlinear PCA Based Face Recognition Techniques, *Int. Arab J. Inf. Technol.*, 10 (2013) pp. 536-545.
17. J.M. Colores-Vargas, M. García-Vázquez, A. Ramírez-Acosta, H. Pérez-Meana, M. NakanoMiyatake, Video images fusion to improve iris recognition accuracy in unconstrained environments, *Mexican Conference on Pattern Recognition*, Springer (2013), pp. 114-125.
18. F. Bokhari, T. Syedia, M. Sharif, M. Yasmin, S.L. Fernandes, Fundus image segmentation and feature extraction for the detection of glaucoma: a new approach, *Current Medical Imaging Reviews*, 14 (2018), pp. 77-87.
19. P. Cofta, H. Lacohee, Understanding public perceptions: trust and engagement in ICT-mediated services, *Intl. Engineering Consortiu*, (2008).
20. A. Panwar, P. Singla, M. Kaur, Techniques for Enhancing the Security of Fuzzy Vault: A Review, *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, Springer, (2018), pp. 205-213.
21. A. Manickam, E. Devarasan, G. Manogaran, M.K. Priyan, R. Varatharajan, C.-H. Hsu, R. Krishnamoorthi, Score level based latent fingerprint enhancement and matching using SIFT feature, *Multimedia Tools and Applications*, (2018), pp. 1-21.
22. M. Sharif, F. Naz, M. Yasmin, M.A. Shahid, A. Rehman, Face Recognition: A Survey, *Journal of Engineering Science & Technology Review*, 10 (2017).

23. J. Hussain Shah, M. Sharif, M. Raza, M. Murtaza, S. Ur-Rehman, Robust Face Recognition Technique under Varying Illumination, *Journal of applied research and technology*, 13 (2015), pp. 97-105.
24. J.H. Shah, M. Sharif, M. Raza, A. Azeem, Face recognition across pose variation and the 3S problem, *turkish journal of electrical engineering & computer sciences*, 22 (2014), pp. 1423-1436.
25. A. Aisha, S. Muhammad, S.J. Hussain, R. Mudassar, Face recognition invariant to partial occlusions, *KSII Trans. Internet Inf. Syst.((TIIS))*, 8 (2014), pp. 2496-2511.
26. M. Murtaza, M. Sharif, M. Raza, J. Shah, Face recognition using adaptive margin fisher's criterion and linear discriminant analysis, *International Arab Journal of Information Technology*, 11 (2014), pp. 1-11.
27. M. Sharif, J.H. Shah, S. Mohsin, M. Raza, Facial Feature Detection and Recognition for Varying Poses, *World Congress on Engineering and Computer Science* (2014), pp. 22-24.
28. A. Azeem, M. Sharif, M. Raza, M. Murtaza, A survey: Face recognition techniques under partial occlusion, *Int. Arab J. Inf. Technol.*, 11 (2014), pp. 1-10.
29. M. Sharif, A. Khalid, M. Raza, S. Mohsin, Face detection and recognition through hexagonal image processing, *Sindh University Research Journal-SURJ (Science Series)*, 44 (2012).
30. M. Sharif, S. Mohsin, M.Y. Javed, A survey: face recognition techniques, *Research Journal of Applied Sciences, Engineering and Technology*, 4 (2012), pp. 4979-4990.
31. M. Sharif, S. Mohsin, M.Y. Javed, M.A. Ali, Single Image Face Recognition Using Laplacian of Gaussian and Discrete Cosine Transforms, *Int. Arab J. Inf. Technol.*, 9 (2012), pp. 562-570.
32. M. Sharif, M.Y. Javed, S. Mohsin, Face recognition based on facial features, *Research Journal of Applied Sciences, Engineering and Technology*, 4 (2012), pp. 2879-2886.
33. M. Sharif, K. Ayub, D. Sattar, M. Raza, S. Mohsin, Enhanced and fast face recognition by hashing algorithm, *Journal of applied research and technology*, 10 (2012), pp. 607-617.

34. M. Sharif, S. Anis, M. Raza, S. Mohsin, Enhanced SVD Based Face Recognition, *Journal of Applied Computer Science & Mathematics*, (2012).
35. M. Sharif, A. Khalid, M. Raza, S. Mohsin, Face Recognition using Gabor Filters, *Journal of Applied Computer Science & Mathematics*, (2011).
36. M. Sharif, S. Mohsin, R.A. Hanan, M.Y. Javed, M. Raza, Using nose heuristics for efficient face recognition, *Sindh University Research Journal-SURJ (Science Series)*, 43 (2011).
37. M. Sharif, S. Mohsin, M.J. Jamal, M.Y. Javed, M. Raza, Face recognition for disguised variations using gabor feature extraction, *Australian Journal of Basic and Applied Sciences*, 5 (2011), pp. 1648-1656.
38. M. Sharif, S. Mohsin, M.J. Jamal, M. Raza, Illumination Normalization Preprocessing for face recognition, *Environmental Science and Information Application Technology (ESIAT)*, 2010 International Conference on, (IEEE2010), pp. 44-47.
39. D.P. Chowdhury, S. Bakshi, G. Guo, P.K. Sa, On applicability of tunable filter bank based feature for ear biometrics: a study from constrained to unconstrained, *Journal of medical systems*, 42 (2018), 11 p.
40. D. Zhang, G. Lu, L. Zhang, Online 3D Ear Recognition, *Advanced Biometrics*, (Springer, 2018), pp. 309-328.
41. M. Boczek, Ear biometric capture, authentication, and identification method and system, *Google Patents* (2017).
42. I.B. Barbosa, T. Theoharis, A.E. Abdallah, On the use of fingernail images as transient biometric identifiers, *Machine Vision and Applications*, 27 (2016), pp. 65-76.
43. A. Uhl, P. Wild, Footprint-based biometric verification, *Journal of Electronic Imaging*, 17 (2008), pp. 11-16.
44. X. Wang, H. Wang, Q. Cheng, N.L. Nankabirwa, T. Zhang, Single 2D pressure footprint based person identification, *Biometrics (IJCB)*, 2017 IEEE International Joint Conference on, (IEEE2017), pp. 413-419.
45. A. Brown, DNA as an investigative technique, *Science and Justice*, 38 (1998), pp. 263-265.
46. C. Forr, B. Schei, L.E. Stene, K. Ormstad, C.T. Hagemann, Factors associated

with trace evidence analyses and DNA findings among police reported cases of rape, *Forensic science international*, 283 (2018), pp. 136-143.

47. M. Shirasu, K. Touhara, The scent of disease: volatile organic compounds of the human body related to disease and disorder, *The Journal of Biochemistry*, 150 (2011), pp. 257-266.

48. S. Haze, Y. Gozu, S. Nakamura, Y. Kohno, K. Sawano, H. Ohta, K. Yamazaki, 2-Nonenal newly found in human body odor tends to increase with aging, *Journal of investigative dermatology*, 116 (2001), pp. 520-524.

49. C.M. Travieso, J. Zhang, P. Miller, J.B. Alonso, M.A. Ferrer, Bimodal biometric verification based on face and lips, *Neurocomputing*, 74 (2011), pp. 2407-2410.

50. Y. Vasquez, C. Beltrán, M. Gómez, M. Flórez, J.L. Vázquez-González, Features extraction in images on finger veins with hybrid curves, *Humanitarian Technology Conference (MHTC), IEEE Mexican, (IEEE2017)*, pp. 34-38.

51. W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, A fingerprint and finger-vein based cancelable multi-biometric system, *Pattern Recognition*, 78 (2018), pp. 242-251.

52. P. Gupta, S. Srivastava, P. Gupta, An accurate infrared hand geometry and vein pattern based authentication system, *Knowledge-Based Systems*, 103 (2016), pp. 143-155.

53. E.J. Esekhaigbe, *Contributions to Biometric Recognition: Fingerprint For Identity Verification*, Cardiff Metropolitan University, (2016).

54. D.-H. Park, B.J. Park, J.-M. Kim, Hydrochromic approaches to mapping human sweat pores, *Accounts of chemical research*, 49 (2016), pp. 1211-1222.

55. A. Genovese, E. Munoz, V. Piuri, F. Scotti, G. Sforza, Towards touchless pore fingerprint biometrics: a neural approach, *Evolutionary Computation (CEC), 2016 IEEE Congress on, (IEEE2016)*, pp. 4265-4272.

56. M.-j. Kim, W.-Y. Kim, J. Paik, Optimum Geometric Transformation and Bipartite Graph-Based Approach to Sweat Pore Matching for Biometric Identification, *Symmetry*, 10 (2018), 175 p.

57. P. Campisi, D. La Rocca, Brain waves for automatic biometric-based user recognition, *IEEE transactions on information forensics and security*, 9 (2014), pp. 782-800.

58. S. Romero, M. Mañanas, M. Barbanoj, Ocular reduction in EEG signals based on adaptive filtering, regression and blind source separation, *Annals of biomedical engineering*, 37 (2009), pp. 176-191.
59. K. Phua, J. Chen, T.H. Dat, L. Shue, Heart sound as a biometric, *Pattern Recognition*, 41 (2008), pp. 906-919.
60. M.S.N. Dere, A. Gurjar, Identification of Human using Palm-Vein Images: A new trend in biometrics, *International Journal Of Engineering And Computer Science* ISSN, 2319-7242.
61. V.S. Nalwa, Automatic on-line signature verification, *Proceedings of the IEEE*, 85 (1997), pp. 215-239.
62. D.B.S. Netto, M. Fornazin, M.A. Cavenaghi, R. Spolon, R.S. Lobato, A practical approach for biometric authentication based on smartcards, *Information Systems and Technologies (CISTI), 2010 5th Iberian Conference*, (2010), pp. 1-5.
63. M. Sharif, M.A. Khan, M. Faisal, M. Yasmin, S.L. Fernandes, A framework for offline signature verification system: Best features selection approach, *Pattern Recognition Letters*, (2018).
64. K.S.R. Murty, B. Yegnanarayana, Combining evidence from residual phase and MFCC features for speaker recognition, *IEEE signal processing letters*, 13 (2006), pp. 52-55.
65. N. Almaadeed, A. Aggoun, A. Amira, Speaker identification using multimodal neural networks and wavelet analysis, *IET Biometrics*, 4 (2015), pp. 18-28.
66. L. Lu, L. Liu, M.J. Hussain, Y. Liu, I sense you by Breath: Speaker Recognition via Breath Biometrics, *IEEE Transactions on Dependable and Secure Computing*, (2017), pp. 1-15.
67. J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, Y. Lee, BreathPrint: Breathing acoustics-based user authentication, *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, (ACM2017), pp. 278-291.
68. M. Raza, M. Iqbal, M. Sharif, W. Haider, A survey of password attacks and comparative analysis on methods for secure authentication, *World Applied Sciences*

Journal, 19 (2012), pp. 439-444.

69. M. Sharif, T. Faiz, M. Raza, Time signatures-an implementation of keystroke and click patterns for practical and secure authentication, Digital Information Management, 2008. ICDIM 2008. Third International Conference on, (IEEE2008), pp. 559-562.
70. M.H. Khan, F. Li, M.S. Farid, M. Grzegorzec, Gait recognition using motion trajectory analysis, International Conference on Computer Recognition Systems, (Springer2017), pp. 73-82.
71. S. Yu, H. Chen, Q. Wang, L. Shen, Y. Huang, Invariant feature extraction for gait recognition using only one uniform model, Neurocomputing, 239 (2017), pp. 81-93.
72. S.D. Choudhury, T. Tjahjadi, Clothing and carrying condition invariant gait recognition based on rotation forest, Pattern Recognition Letters, 80 (2016), pp. 1-7.
73. J.N. Mogan, C.P. Lee, A.W. Tan, Gait recognition using temporal gradient patterns, Information and Communication Technology (ICoIC7), 2017 5th International Conference on, (IEEE2017), pp. 1-4.
74. S. Tao, X. Zhang, H. Cai, Z. Lv, C. Hu, H. Xie, Gait based biometric personal authentication by using MEMS inertial sensors, Journal of Ambient Intelligence and Humanized Computing, (2018), pp. 1-8.
75. A. Byrnes, A. Mudge, A. Young, M. Banks, J. Bauer, Use of hand grip strength in nutrition risk screening of older patients admitted to general surgical wards, Nutrition & Dietetics, (2018).
76. A. Wichelhaus, C. Harms, J. Neumann, S. Ziegler, G. Kundt, K.J. Prommersberger, T. Mittlmeier, M. Mühldorfer-Fodor, Parameters influencing hand grip strength measured with the manugraphy system, BMC musculoskeletal disorders, 19 (2018), 54 p.
77. M.S. Islam, M. Ali, K.H. Zubaer, S. Sarmin, M.T. Islam, B. Islam, A.A. Al Islam, A.M. Sadri, Trusted Worrier: A low-cost and high-accuracy user authentication system for firearm exploiting dynamic hand pressure biometrics, Networking, Systems and Security (NSysS), 2017 International Conference on, (IEEE2017), pp. 87-95.
78. Jain, A. K., Nandakumar, K., and Nagar, A. Biometric template security.

EURASIP J. Adv. Signal Process (2008).

79. Kim, W., and Lee, H. Multimodal biometric image watermarking using two-stage integrity verification. *Signal Processing* 89, 2 (2009), pp. 2385-2399.
80. Yang, S., and Verbaauwhede, I. M. A secure fingerprint matching technique. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, WBMA '03*, ACM, New York, (2003), pp. 89–94.
81. Liu, L., Yang, J., Chaozhe, Z., and Jiang, T. Information theory based fingerprint matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2011).
82. Wikipedia. Minutiae. URL: <http://en.wikipedia.org//index.php?title=Minutiae&oldid=359363333>.
83. Вікіпедія. Позиційний кут. URL: <http://surl.li/oymvd>.
84. L. A. Hornak, The Center for Identification Technology Research, Summary, An IUCRC Planning Grant Proposal, West Virginia University, Michigan State University and San Jose State University & Marshall University.
85. A. Corradini, M. Mehta, N. O. Bernsen, J. C. Martin, S. Abrilian, Multimodal Input Fusion in HumanComputer Interaction, On the Example of the NICE Project, (2003).
86. N. Poh and S. Bengio, Database, Protocol and Tools for Evaluating Score-Level Fusion Algorithms in Biometric Authentication, (Switzerland), (2004).
87. J. Matas, M. Hamouz, K. Jonsson, J. Kittler, Y. Li, C. Kotropoulos, A. Tefas, I. Pitas, T. Tan, H. Yan, F. Smeraldi, J. Begun, N. Capdevielle, W. Gerstner, S. Ben-Yacoub, Y. Abdeljaoued and E. Mayoraz, Comparison of Face Verication Results on the XM2VTS Database, In *Proc. 15th Int'l Conf. Pattern Recognition*, vol. 4, (Barcelona), (2000), pp. 858-863.
88. E. Bailly-Bailliere, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz, J. Matas, K. Messer, V. Popovici, F. Poree, B. Ruiz and J. -P. Thiran, The BANCA database and evaluation protocol, in *Proc. Audioand Video-Based Biometric Person Authentication*, (Guilford), (2003), pp. 625-638.
89. P. S. Aleksic and A. K. Katsaggelos, Audio-Visual Biometrics, *Proceedings of the IEEE*, vol. 94, no. 11, (2006).

90. C. Sanderson and K. K. Paliwal, Noise compensation in a person verification system using face and multiple speech features, *Pattern Recognition*, vol. 36, no. 2, (2003), pp. 293–302.
91. C. Sanderson and K. K. Paliwal, Identity verification using speech and face information, *Digital Signal Processing*, vol. 14, no. 5, (2004), pp. 449-480.
92. S. Marcel and S. Bengio, Improving Face Verification Using Skin Color Information, In *Proc. 16th Int. Conf. on Pattern Recognition*, (Quebec), (2002).
93. C. Sanderson and K. K. Paliwal, Fast Features for Face Authentication Under Illumination Direction Changes, *Pattern Recognition Letters*, vol. 24, no. 14, (2003), pp. 2409-2419.
94. L. Rabiner and B. -H. Juang, *Fundamentals of Speech Recognition*, Oxford University Press, (1993).
95. S. Ikbali, H. Misra and H. Bourlard, Phase Auto-Correlation (PAC) derived Robust Speech Features, In *Proc. IEEE Int'l Conf. Acoustics, Speech, and Signal Processing (ICASSP-03)*, (Hong Kong), (2003), pp. 133-136.
96. K. K. Paliwal, Spectral Subband Centroids Features for Speech Recognition, In *Proc. Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, vol. 2, (Seattle), (1998), pp. 617-620.
97. N. Poh, C. Sanderson and S. Bengio, An Investigation of Spectral Subband Centroids For Speaker Authentication, In *Springer LNCS-3072, Int'l Conf. on Biometric Authentication (ICBA)*, (Hong Kong), (2004), pp. 631-639.
98. F. Cardinaux, C. Sanderson and S. Marcel, Comparison of MLP and GMM Classifiers for Face Verification on XM2VTS, In *Springer LNCS-2688, 4th Int'l Conf. Audio- and Video-Based Biometric Person Authentication (Guildford)*, (2003), pp. 911-920.
99. N. Poh and S. Bengio, Noise-Robust Multi-Stream Fusion for Text-Independent Speaker Authentication, In *The Speaker and Language Recognition Workshop*, Toledo, (2004), pp. 199-206.
100. T. J. Hazen, E. Weinstein, R. Kabir, A. Park and B. Heisele, Multi-modal face and speaker identification on a handheld device, in *Proc. Works Multimodal User*

Authentication, (Santa Barbara, CA), (2003), pp. 113-120.

101. A. Ross and A. K. Jain, Multimodal Biometrics: An Overview, Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna), (2004), pp. 1221-1224.

102. A. A. Ross, A. K. Jain, and K. Nandakumar, Information fusion in biometrics, Handbook of Multibiometrics, (2006), pp. 37-58.

103. A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of multibiometrics vol. 6: Springer Science & Business Media, (2006).

104. K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. KailasaRao, Multimodal biometric systems study to improve accuracy and performance, 2010.

105. L. Latha and S. Thangasamy, A robust person authentication system based on score level fusion of left and right irises and retinal features, Procedia Computer Science, vol. 2, (2010), pp. 111-120.

106. Y. Wang, T. Tan, and A. K. Jain, Combining face and iris biometrics for identity verification, International Conference on Audio-and Video-Based Biometric Person Authentication, (2003), pp. 805-813.

107. S. C. Dass, K. Nandakumar, and A. K. Jain, A principled approach to score level fusion in multimodal biometric systems, International conference on audio-and video-based biometric person authentication, (2005), pp. 1049-1058.

108. W. Scheirer, A. Rocha, R. Micheals, and T. Boulton, Robust fusion: Extreme value theory for recognition score normalization, European Conference on Computer Vision, (2010), pp. 481-495.

109. M. M. Hamdi, L. Audah, S. A. Rashid, S. Alani, M. A. Al-Mashhadani, and A. S. Mustafa, Green Communication Networks Challenges, Opportunities and Future Role, Journal of Communications, vol. 15, (2020), pp. 256-262.

110. A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature, International Journal of Computer Applications, vol. 2, (2010), 16-26.

111. A. J. Basha, V. Palanisamy, and T. Purusothaman, Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features,

Second Journal of Computer Science, (2011).

112. M. Abdolahi, M. Mohamadi, and M. Jafari, Multimodal biometric system fusion using fingerprint and iris with fuzzy logic, International Journal of soft computing and engineering, vol. 2, (2013), pp. 504-510.

113. L.-q. Zhu and S.-y. Zhang, Multimodal biometric identification system based on finger geometry, knuckle print and palm print, Pattern Recognition Letters, vol. 31, (2010), pp. 1641-1649.

114. S. Ghorpade, D. Gund, S. Kadam, and M. R. Jamadar, Image Quality Assessment for Fake Biometric Detection: Application to Face and Fingerprint Recognition, International Journal of Emerging Technologies and Engineering (IJETE), vol. 2, (2015).

115. S. Zhang, H. Wang, and W. Huang, Two-stage plant species recognition by local mean clustering and Weighted sparse representation classification, Cluster computing, vol. 20, (2017), pp. 1517-1525.

116. S. Bakshi, P. K. Sa, H. Wang, S. S. Barpanda, and B. Majhi, Fast periocular authentication in handheld devices with reduced phase intensive local pattern, Multimedia Tools and Applications, vol. 77, (2018), pp. 17595-17623.

117. A. Adamu. Attendance management system using fingerprint and iris biometric. Fudma Journal of Sciences-ISSN: 2616-1370, vol. 3, (2020), pp. 427-433.

118. Вікіпедія. Система контролю і управління доступом. URL: <http://surl.li/drnngn>.

119. ZKTeco. Biometric Reader. URL: <https://www.zkteco.com/en/BiometricReader>.

120. ZKTeco. Biometric Control Panel. URL: <https://www.zkteco.com/en/BiometricControlPanelOAh>.

121. ZKTeco. Biometrics Terminal. URL: <https://www.zkteco.com/en/BiometricsTerminal>.

122. ZKTeco. Company Profile. URL: <https://www.zkteco.com/en/about>.

123. Wikipedia. Face ID. URL: https://en.wikipedia.org/wiki/Face_ID.

124. Innovatrics. Liveness Detection. URL: <https://www.innovatrics.com/glossary/liveness-detection/>.